

DESCRIPTION**KEY DISTRIBUTION SYSTEM****Technical Field**

5 [0001] The present invention relates to a key distribution system which distributes shared keys to receiving devices. It especially relates to a technique which enables tracing a receiving device which is a leakage source, in the case where the information which is assigned to the receiving device is leaked, by making the
10 information which is necessary for obtaining a shared key unique to each receiving device.

Background Art

15 [0002] With the widespread use of high-speed communication channels represented by ADSL, optical fiber and the like, services for providing contents including digital music and video through such communication channels have been actively provided. With the prevalence of such services, a copyright protection method for preventing an unauthorized use of contents, represented by an
20 unauthorized copying, has become necessary. As a copyright protection method for preventing an unauthorized use of contents, an encryption technique is generally used. In other words, with the encryption technique, digital contents are encrypted using a content encryption key and distributed through a communication channel,
25 which enables only the receiving devices to decrypt the encrypted contents and to play back the original digital contents, the receiving devices with a content decryption key corresponding to the content encryption key.

30 [0003] By the way, the content decryption keys which have been provided to the receiving devices are generally held in secret. However, there is a possibility that an attacker will obtain a content decryption key which has been provided to all the receiving devices

in common by analyzing a device in an unauthorized manner. Once the content decryption key provided to a certain receiving device has been leaked, the attacker may create an unauthorized receiving device which decrypts digital contents using the content decryption
5 key based on which the leakage source cannot be traced and may use the contents in an unauthorized manner. As one of the countermeasures for preventing such an unauthorized use of contents, there is a conceivable system where the receiving device which is a leakage source can be traced by providing an individual
10 key to each receiving device. As an example method for preventing an unauthorized use of contents in broadcasting station style content distribution where the same data is sent to all the receiving devices, there is a key distribution system described in the following Non-patent Reference 1.

15 [0004] FIG. 53 shows a conventional key distribution system described in the Non-patent Reference 1. In FIG. 53, a communication channel 90 is a communication channel which connects the key distribution center 91, the server 92 and receiving devices 93a to 93n which will be described later, and is realized by
20 means of a network such as the Internet and a broadcasting network. Also, each pair of the key distribution center 91 and the respective one of receiving devices 93a to 93n previously shares the corresponding one of the individual keys IKa to IKn. For example, it is assumed that the key distribution center 91 and the receiving
25 device 93a previously share the individual key IKa, the key distribution center 91 and the receiving device 93b previously share the individual key IKb, and the key distribution center 91 and the receiving device 93n previously share the individual key IKn.

30 [0005] First, here will be described the method where all the respective receiving devices 93a to 93n have shared intermediate keys SMK with a same value. The key distribution center 91 generates shared intermediate keys SMK and sends the shared

intermediate keys SMK to the server 92. Next, the key distribution center 91 encrypts the shared intermediate keys SMK based on the individual keys IKa, IKb, ..., IKn which have been previously shared with the respective receiving devices 93a to 93n, and distributes encrypted shared intermediate key groups with a same value to the receiving devices 93a to 93n, the group being $ENCSMKG = \text{Enc}(IKa, SMK) || \text{Enc}(IKb, SMK) || \dots \text{Enc}(IKn, SMK)$ which is the value obtained by combining the encrypted sentences of $\text{Enc}(IKa, SMK)$, $\text{Enc}(IKb, SMK)$, ..., and $\text{Enc}(IKn, SMK)$ with each other. Here, "||" is a
connective, and $\text{Enc}(K, P)$ indicates an encrypted sentence obtained at the time when a plane sentence P is encrypted using an encryption key K. Note that in the Non-patent Reference 1, the encrypted shared intermediate key group ENCSMKG is referred to as individual information (EMM), the individual keys IKa to IKn are referred to as master key (Km), and the shared intermediate key SMK is referred to as work key (Kw) respectively. Each of the receiving devices 93a to 93n which have received the encrypted shared intermediate key group ENCSMKG extracts the encrypted sentence corresponding to the local individual key from among the encrypted shared intermediate key group ENCSMKG, decrypts the encrypted sentence based on the individual key and obtains the shared intermediate key SMK. In this way, all the receiving devices 93a to 93n can have the shared intermediate keys SMK with a same value.

[0006] Next, the method where all the respective receiving devices 93a to 93n have shared keys SK which are used at the time of decrypting contents or the like will be described. The server 92 generates shared keys SK, encrypts the shared keys SK based on the shared intermediate keys SMK which are owned by the receiving devices 93a to 93n, and distributes the encrypted sentences $\text{Enc}(SMK, SK)$ as encrypted shared keys ENCSK to the receiving devices 93a to 93n. The receiving devices 93a to 93n which have

received the encrypted shared keys ENCSK decrypt the encrypted shared keys ENCSK based on the shared intermediate keys SMK and obtain shared keys SK respectively. In this way, all the receiving devices 93a to 93n can have the shared keys SK. Note that, in the Non-patent Reference 1, the shared key SK is referred to as scramble key (Ks), and the encrypted shared key ENCSK is referred to as common information (ECM) respectively. Note that it is possible to update to new shared keys SK by means that the server 92 generates encrypted shared keys ENCSK based on the new shared keys SK and distributes the encrypted shared keys ENCSK to the receiving devices 93a to 93n.

[0007] Note that the key distribution center 91 can also disable the receiving device which has a specific individual key in order to prevent the receiving device from obtaining the shared keys SK. Here, the case of disabling the receiving device which has the individual key of the receiving device 93a will be described. First, shared intermediate keys SMK are newly generated, and the shared intermediate keys SMK are sent to the server 92. After that, the shared intermediate keys SMK are encrypted using all the respective individual keys IKb to IKn excluding the individual key IKa which is previously shared with the receiving device 93a, and distributes encrypted shared intermediate key groups with a same value to the receiving devices 93a to 93n, the value being $ENCSMKG = \text{Enc}(IKb, SMK) || \dots || \text{Enc}(IKn, SMK)$ which is the value obtained by combining the encrypted sentences of $\text{Enc}(IKb, SMK)$, ..., and $\text{Enc}(IKn, SMK)$ with each other. In this way, the receiving devices 93b to 93n excluding the receiving device 93a can obtain the shared keys SK because they can obtain the shared intermediate keys SMK, but the receiving device 93a cannot obtain the shared keys SK because it cannot obtain the shared intermediate keys SMK. In this way, the key distribution center 91 can disable the receiving device. In the case where the receiving devices 93b to 93n, excluding the receiving

device 93a, are disabled, it should be noted that the same operation as the one in the case of the receiving device 93a is executed, however there is a difference that another individual key is used at the time of encrypting the shared intermediate key SMK.

5 [0008] With the system like this, it is possible to trace the receiving device which is a leakage source based on the individual key which has been embedded in the receiving device, even in the case where an attacker obtains the individual key which has been embedded in one of the receiving devices 93a to 93n in an
10 unauthorized manner and creates a receiving device using the individual key, and thus it becomes possible to take a countermeasure such as disabling the target receiving device.

Non-patent Reference 1: "The Mechanism of Digital Broadcasting System", edited by The Institute of Image Information and
15 Television Engineers, and published by Ohmsha-Press.

Non-patent Reference 2: "Gendai angouriron (Modern Cryptosystem)", co-written by Shinichi Ikeno and Kenji Koyama, edited by the Institute of Electronics, Information and Communication Engineers.

20 Non-patent Reference 3: THE ART OF COMPUTER PROGRAMMING Vol. 2 ~ SEMINUMERICAL ALGORITHMS, DONALD E. KNUTH, ISBN 0-201-03822-6.

Disclosure of Invention

25 Problem to be Solved

[0009] In addition to the earlier-described method, the following case is conceivable in the case where the individual key which has been embedded in one of the receiving devices 93a to 93n is obtained in an unauthorized manner: the case where an attacker
30 obtains a shared intermediate key SMK using the individual key and creates an unauthorized receiving device in which the shared intermediate key SMK is embedded. The earlier-described

configuration had a problem that the receiving device as the leakage source cannot be traced based on the key (shared intermediate key SMK) embedded in the unauthorized receiving device when facing such an attack because all the receiving devices 93a to 93n have the shared intermediate keys SMK with a same value.

[0010] The present invention has been conceived in order to solve the above-described problem. An object of the present invention is to provide a key distribution system where the receiving device which is a leakage source can be traced even in the case where an attacker creates an unauthorized receiving device in which an intermediate key is embedded.

Means for Solving the Problem

[0011] A key distribution system for distributing shared keys includes: a server which generates common information based on each of the shared keys and distributes the common information; and receiving devices each of which obtains the shared key based on the common information and an individual intermediate key group set. In the key distribution system, each of the receiving devices has been previously provided with at least one individual intermediate key group set which has been selected from among individual intermediate key group sets including at least two different types of individual intermediate key group sets. Each of the individual intermediate key group sets includes individual intermediate key groups, and each of the individual intermediate key groups is made up of one or more individual intermediate keys which have been generated based on one or more system secret variable groups. In the key distribution system, the server and the receiving devices can communicate via a communication channel. The server includes: a shared key storage unit which stores the shared keys; a system secret variable group storage unit which stores the system secret variable group sets which are made up of

the previously provided system secret variable groups; each of common information generation units which generates the common information based on each shared key; a common information generation unit selection unit which selects one of the common information generation units; and a common information distribution unit which distributes the common information to the receiving devices simultaneously or at different times, each of the common information generation units which generates key update data based on the system secret variable group set and the shared key and generates, using a different common information generation method, common information including (a) a common information identifier and (b) the key update data, the common information identifier corresponding to the common information generation method. Each of the receiving devices include: a common information receiving unit which receives the common information; an individual intermediate key group storage unit which stores the individual intermediate key group sets each of which is made up of the individual intermediate key groups corresponding to each of the common information generation methods; shared key obtainment units which respectively correspond to the common information generation units; and a shared key obtainment unit selection unit which selects one of the shared key obtainment units. The shared key obtainment unit selection unit selects one of the shared key obtainment units based on the common information identifier included in the common information which has been received by the common information receiving unit. Each of the shared key obtainment units obtains the shared key, using the common information, based on the shared key obtainment method corresponding to the common information identifier and the individual intermediate key group.

[0012] In a first aspect of the present invention, in the key distribution system, each common information generation method

includes a first common information generation method. Each shared key obtainment method includes a first shared key obtainment method which is paired with the first common information generation method. Each of the system secret variable group sets includes first system secret variable groups each of which is made up of one or more first system secret variables. Each of the individual intermediate key group sets includes first individual intermediate key groups each of which is made up of one or more first individual intermediate keys, the first individual intermediate keys are respectively generated based on the first system secret variable groups and one or more first individual intermediate key generation equations. The server has been previously provided with one or more time variable generation equations and one or more server shared intermediate key generation equation. Each of the receiving devices has been previously provided with one or more receiving device shared intermediate key generation equations. The first common information generation method includes: generating a random number group which is made up of one or more random numbers; generating a time variable group which is made up of one or more time variables based on the random number group, the first system secret variable groups and the time variable generation equations; generating shared intermediate keys based on the first system secret variable groups, the random number group and the server shared intermediate key generation equations; and generating encrypted shared keys by encrypting the shared keys based on the shared intermediate keys. In the first common information generation method, the key update data includes the time variable group and the encrypted shared keys. The first shared key obtainment method includes: generating the shared intermediate keys based on the time variable group, the first individual intermediate key group and the receiving device shared intermediate key generation equations; and obtaining the shared

keys by decrypting the encrypted shared keys based on the shared intermediate keys.

[0013] In the first aspect of the present invention, in the key

distribution system, the server has been previously provided with

5 one of the individual intermediate key group sets. The server

includes an individual intermediate key group set storage unit which

stores the previously provided individual intermediate key group set.

Each common information generation method includes a first

common information generation method, and each shared key

10 obtainment method includes a first shared key obtainment method

which is paired with the first common information generation

method. Each of the system secret variable group sets includes

first system secret variable groups each of which is made up of one

or more first system secret variables. Each of the individual

15 intermediate key group sets includes first individual intermediate

key groups each of which is made up of one or more first individual

intermediate keys, the first individual intermediate keys are

respectively generated based on the first system secret variable

groups and one or more first individual intermediate key generation

20 equations. The server has been previously provided with one or

more time variable generation equations and one or more server

shared intermediate key generation equation. Each of the

receiving devices has been previously provided with one or more

receiving device shared intermediate key generation equations. The

25 first common information generation method includes: generating a

random number group which is made up of one or more random

numbers; generating a time variable group which is made up of one

or more time variables based on the random number group, the first

system secret variable groups and the time variable generation

30 equations; generating shared intermediate keys based on the first

system secret variable groups, the random number group and the

server shared intermediate key generation equations; and

generating encrypted shared keys by encrypting the shared keys based on the shared intermediate keys. In the first common information generation method, the key update data includes the time variable group and the encrypted shared keys. The first
5 shared key obtainment method includes: generating the shared intermediate keys based on the time variable group, the first individual intermediate key group and the receiving device shared intermediate key generation equations; and obtaining the shared keys by decrypting the encrypted shared keys based on the shared
10 intermediate keys.

[0014] In the first aspect of the present invention, in the key distribution system, each common information generation method includes a second common information generation method, and each shared key obtainment method includes a second shared key
15 obtainment method which is paired with the second common information generation method. Each of the system secret variable group sets includes a second system secret key group which is made up of second system secret keys, and each of the individual intermediate key group sets includes second individual intermediate
20 key groups each of which is made up of one or more of the second system secret keys. The second common information generation method includes: generating encrypted shared keys by encrypting the shared keys based on one or more of the second system secret keys which are included in the second system secret key groups;
25 and generating an encrypted shared key group which is made up of the encrypted shared keys combined with each other. In the second common information generation method of the key distribution system, the key update data includes the encrypted shared key group. The second shared key obtainment method
30 includes: selecting one of the encrypted shared keys which corresponds to any of the second system secret keys included in the second individual intermediate key group, from among the

encrypted shared key group included in the key update data; and obtaining the shared key by decrypting the selected encrypted shared key based on the second system secret key.

[0015] In the forth aspect of the present invention, in the key distribution system, the individual intermediate key group set includes a second individual intermediate key group which is made up of one of the second system secret keys. The second common information generation method includes: generating encrypted shared keys by encrypting the shared keys based on the second system secret keys which are included in the second system secret key group; and generating an encrypted shared key group which is made up of encrypted shared keys combined with each other.

[0016] In the first aspect of the present invention, the key distribution system, further includes a key distribution center which is connected with the respective receiving devices via the communication channel and distributes an individual information group. The key distribution center, in the key distribution system, includes: an output device information storage unit which stores one or more individual keys which have been previously provided to the receiving devices; individual information generation units which generates the individual information; and an individual information group distribution unit which distributes the individual information group including at least two types of sets of the individual information and an individual information identifier which corresponds to the individual information generation unit, to the receiving devices simultaneously or at different times. Each of the individual information generation units outputs the individual information identifier, the system secret variable group and the individual information based on the individual information generation method which is uniquely used by each of the individual information generation units. Each of the receiving devices includes: an individual key storage unit which stores the previously

provided individual key; an individual information group receiving unit which receives the individual information group; and individual intermediate key group obtainment units which correspond to the individual information generation units. The individual information group receiving units output the individual information corresponding to the individual information identifiers to the respective individual intermediate key obtainment units based on the individual information identifiers included in the received individual information group. Each of the individual intermediate key obtainment units obtains the individual intermediate key group based on the individual information and the individual key using an individual intermediate key obtainment method corresponding to the individual information identifier.

[0017] In a sixth aspect of the present invention, in the key distribution system, each of the individual information generation units further generates the system secret variable group. The key distribution center includes a system secret variable group set sending unit which distributes, to the server, the system secret variable group set including two types of sets of the system secret variable group and the individual information identifier which corresponds to the individual information generation unit. The server includes a system secret variable group set receiving unit stores the distributed system secret variable group sets into the system secret variable group storage unit.

[0018] In the sixth aspect of the present invention, in the key distribution system, the key distribution center is connected to the server via the communication channel. The system secret variable group set sending unit distributes the system secret variable group set to the server via the communication channel. The system secret variable group set receiving unit receives the system secret variable group set from the key distribution center via the communication channel.

[0019] In the sixth aspect of the present invention, in the key distribution system, the system secret variable group set sending unit records the system secret variable group set on a portable medium, and the system secret variable group set receiving unit
5 reads out the system secret variable group set recorded on the portable medium.

[0020] In a seventh aspect of the present invention, in the key distribution system, the key distribution center and the server are assumed to share a server key in advance. The system secret variable group set sending unit generates encrypted data by
10 encrypting the system secret variable group set based on the server key and distribute the server key to the server. The system secret variable group set receiving unit obtains the system secret variable group set by decrypting the distributed encrypted data based on the
15 server key.

[0021] In the sixth aspect of the present invention, in the key distribution system, each individual information generation method includes a first individual information generation method. Each individual intermediate key obtainment method includes a first
20 individual intermediate key obtainment method which is paired with the first individual information generation method. The key distribution center includes a term information storage unit which stores one or more types of sets of a previously provided term key, a first system secret variable group, and a term identifier, the first
25 system secret variable group and the term identifier corresponding to the term key. The individual key storage units of the receiving devices each stores one or more types of sets of a first encrypted individual intermediate key group and a term identifier, the encrypted first individual intermediate key group is generated by
30 encrypting the first individual intermediate key group based on the term key, and the term identifier corresponding to the term key. The first individual information generation method includes:

selecting a set of a term key, a first system secret variable group and a term identifier which are included in the term information storage unit; and generating encrypted term keys by encrypting the term keys based on each of the individual keys. The individual information group includes first individual information which is composed of an encrypted term key group and the term identifier, and the encrypted term key group is made up of the encrypted term keys combined with each other. The first individual intermediate key group obtainment method includes: obtaining the term key by decrypting one of the encrypted term keys which are included in the first individual information; and selecting the first encrypted individual intermediate key group corresponding to the term identifier from among one or more of the first encrypted individual intermediate key groups included in the individual key storage unit; and obtaining the first individual intermediate key group by decrypting the encrypted first individual intermediate key group based on the term key.

[0022] In the sixth aspect of the present invention, in the key distribution system, each individual information generation method includes a second individual information generation method, and each individual intermediate key obtainment method includes a second individual intermediate key group obtainment method which is paired with the second individual information generation method. The second individual information generation method includes: selecting one of the second system secret keys for each of the individual keys; and generating second encrypted system secret keys by encrypting the selected second system secret key based on each of the individual keys. In the second individual information generation method of the key distribution system, the individual information group includes second individual information including a second encrypted system secret key group which is made up of the second encrypted system secret keys combined with each other.

The second individual intermediate key group obtainment method includes: selecting one second encrypted system secret key corresponding to the individual key from among the second encrypted system secret keys included in the second individual information; and obtaining the second system secret key by decrypting the selected second encrypted system secret key based on the individual key. The second system secret key is considered as the second individual intermediate key group.

[0023] In a second aspect of the present invention, in the key distribution system, the individual intermediate key generation equation includes at least addition operation and multiplication operation.

[0024] In the second aspect of the present invention, in the key distribution system, the time variable generation equation includes at least addition operation and multiplication operation.

[0025] In the second aspect of the present invention, in the key distribution system, the server shared intermediate key generation equation includes at least addition operation and multiplication operation.

[0026] In the second aspect of the present invention, in the key distribution system, the receiving device shared intermediate key generation equation includes at least addition operation and multiplication operation.

[0027] In the forth aspect of the present invention, in the key distribution system, the second system secret key group is made up of ten second system secret keys.

[0028] The receiving device in a key distribution system of the present invention, includes a server which distributes shared keys and receiving devices which receive the shared keys. The receiving devices include: a common information receiving unit which receives the common information from outside; an individual intermediate key group storage unit which stores individual

intermediate key group sets each of which is made up of individual intermediate key groups corresponding to each of the common information generation methods; shared key obtainment units which correspond to the common information generation methods; and a shared key obtainment unit selection unit which selects one of the shared key obtainment units. The shared key obtainment unit selection unit selects the shared key obtainment unit based on the common information identifier included in the common information which has been received by the common information receiving unit. The shared key obtainment unit obtains the shared key, using the common information, based on the shared key obtainment method corresponding to the common information identifier and the individual intermediate key group.

[0029] In an eighteenth aspect of the present invention, in the receiving device, each shared key obtainment method includes a first shared key obtainment method. The individual intermediate key group set includes an individual intermediate key group which is made up of one or more first individual intermediate keys. Each of the receiving devices has been provided with one or more receiving device shared intermediate key generation equations. The common information includes first common information which is made up of a time variable group and an encrypted shared key. The first shared key obtainment method includes: generating the shared intermediate keys based on the time variable group, the first individual intermediate key group and the receiving device shared intermediate key generation equations which are included in the first common information; and obtaining the shared keys by decrypting the encrypted shared keys based on the shared intermediate keys.

[0030] In the eighteenth aspect of the present invention, in the receiving device, each shared key obtainment method includes a second shared key obtainment method. The individual

intermediate key group set includes a second individual intermediate key group which is made up of one or more of the second system secret keys. The common information includes second common information which is made up of an encrypted shared key group including one or more encrypted shared keys, and the encrypted shared keys is generated by encrypting the shared keys based on the one or more of the second system secret keys. The second shared key obtainment method includes: selecting one of the encrypted shared keys which corresponds to any of the second system secret keys included in the second individual intermediate key group from among the encrypted shared key group included in the second common information; and obtaining the shared key by decrypting the selected encrypted shared key based on the second system secret key.

[0031] In a twentieth aspect of the present invention, in the receiving device, the individual intermediate key group set includes a second individual intermediate key group which is made up of one of the second system secret keys.

[0032] In the eighteenth aspect of the present invention, in the receiving device, the key distribution system further includes a key distribution center which is connected with the receiving devices via the communication channel and distributes an individual information group. Each of the receiving devices includes: an individual key storage unit which stores the previously provided individual key; an individual information group receiving unit which receives the individual information group from outside; and individual intermediate key group obtainment units which correspond to the individual intermediate key obtainment methods. The individual information group receiving units output the individual information corresponding to the individual information identifiers included in the individual information group to the respective individual intermediate key obtainment units based on

the individual information identifiers included in the received individual information group. Each of the individual intermediate key obtainment units obtains the individual intermediate key group based on the individual information and the individual key using an individual intermediate key obtainment method corresponding to the individual information identifier.

[0033] In an nineteenth aspect of the present invention, in the receiving device, each individual intermediate key obtainment method includes a first individual intermediate key group obtainment method. Each of the individual key storage units of the receiving devices stores one or more types of sets of a first encrypted individual intermediate key group and a term identifier, and the first encrypted individual intermediate key group is generated by encrypting the first individual intermediate key group based on a term key, and the term identifier corresponding to the term key. The individual information group includes first individual information which is made up of an encrypted term key group and the term identifier, the encrypted term key group including encrypted term keys generated by encrypting the term keys based on the respective individual keys. The first individual intermediate key group obtainment method includes: obtaining the term key by decrypting one of the encrypted term keys included in the first individual information; selecting one of the first encrypted individual intermediate key groups which corresponds to the term identifier from among one or more of the first encrypted individual intermediate key groups included in the individual key storage unit; and obtaining the first individual intermediate key group by decrypting the first encrypted individual intermediate key group based on the term key.

[0034] In the twentieth aspect of the present invention, in the receiving device, each individual intermediate key obtainment method includes a second individual intermediate key group

obtainment method. The individual information group includes second individual information including a second encrypted system secret key group which is made up of second encrypted system secret keys generated by encrypting one of the second system secret keys based on the respective individual keys. The second individual intermediate key group obtainment method includes: selecting one second encrypted system secret key corresponding to the individual key from among the second encrypted system secret keys included in the second individual information; and obtaining the second system secret key by decrypting the selected second encrypted system secret key based on the individual key. The second system secret key is considered as the second individual intermediate key group.

[0035] In the nineteenth aspect of the present invention, in the receiving device, each of the receiving device shared intermediate key generation equations includes at least addition operation and multiplication operation.

[0036] A program, in the present invention, which causes a computer to execute processing of receiving shared keys, and the computer is connected with a server which distributes the shared keys via a communication channel. The processing includes: a reception step of receiving the common information from outside; a storage step of storing an individual intermediate key group set which is made up of individual intermediate key groups corresponding to the respective shared key obtainment methods; an obtainment step of obtaining the shared keys corresponding to the shared key obtainment methods; and a selection step of selecting one of the shared key obtainment units based on the common information identifiers included in the common information which has been received by the common information receiving unit. In the processing, the obtainment step includes the following: obtaining the shared keys, using the common information, based on

the shared key obtainment method and the individual intermediate key group, the shared key obtainment method corresponding to the common information identifier.

[0037] In a twenty-sixth aspect of the present invention, in the program, each shared key obtainment method includes a first shared key obtainment method. The individual intermediate key group set includes a first individual intermediate key group which is made up of one or more first individual intermediate keys. Each of the programs has been previously provided with one or more receiving device shared intermediate key generation equations. The common information includes first common information which is made up of encrypted shared keys generated by encrypting the shared keys based on a time variable group and shared intermediate keys. The first shared key obtainment method includes: generating the shared intermediate keys based on the time variable group included in the first common information, the first individual intermediate key group and the receiving device shared intermediate key generation equations; and obtaining the shared keys by decrypting the encrypted shared keys based on the shared intermediate keys.

[0038] In the twenty-sixth aspect of the present invention, in the program, each shared key obtainment method includes a second shared key obtainment method. The individual intermediate key group set includes a second individual intermediate key group which is made up of one or more of the second system secret keys. The common information includes second common information including an encrypted shared key group which is made up of encrypted shared keys. The encrypted shared keys are generated by encrypting the shared keys based on one or more of the second system secret keys. The second shared key obtainment method includes: selecting one of the encrypted shared keys which corresponds to any of the second system secret keys included in the

second individual intermediate key group from among the encrypted shared key group which is included in the second common information; and obtaining the shared key by decrypting the selected encrypted shared key based on the second system secret
5 key.

[0039] In a twenty-eighth aspect of the present invention, in the program, the individual intermediate key group includes one of second individual intermediate key groups each of which is made up of one of the second system secret keys.

10 [0040] In a twenty-seventh aspect of the present invention, in the program, each of the receiving device shared intermediate key generation equations includes at least addition operation and multiplication operation.

[0041] The program in a twenty sixth aspect is recorded on a
15 medium of the present invention.

[0042] A key distribution method of the present invention includes: a key distribution step of generating common information based on each of the shared keys and distributing the common information; and key reception steps of obtaining the shared keys
20 based on the common information and an individual intermediate key group set. In the key reception steps of the key distribution method, at least one individual intermediate key group set has been previously provided. In the key distribution method, the individual intermediate key group set has been selected from among individual
25 intermediate key group sets including at least two different types of individual intermediate key group sets. Each of the individual intermediate key group sets includes individual intermediate key groups, and each of the individual intermediate key groups is made up of one or more individual intermediate keys which have been
30 generated based on one or more system secret variable groups. The key distribution step includes: a shared key storage step of storing the shared keys; a storage step of storing the system secret

variable group sets which are made up of the previously provided system secret variable groups; generation steps of generating common information based on each shared key; a selection step of selecting one of the common information generation steps; and a distribution step of distributing the common information to the receiving devices simultaneously or at different times. The common information generation steps are generating, using different common information generation methods respectively, key update data based on the system secret variable group set and the shared key and generating common information including (a) common information identifiers and (b) the key update data, the common information identifiers respectively corresponding to the common information generation methods. The key reception steps include: a reception step of receiving the common information; a storage step of storing the individual intermediate key group sets each of which is made up of the individual intermediate key groups respectively corresponding to the common information generation methods; obtainment steps of obtaining shared keys, the steps respectively corresponding to the generation units which generate common information; and a selection step of selecting one of the shared key obtainment steps based on the common information identifiers included in the common information which has been received by the common information reception units. The obtainment steps include obtaining, the shared keys, using the common information based on (a) the shared key obtainment methods respectively corresponding to the common information identifiers and (b) the individual intermediate key group.

[0043] In a thirty-second aspect of the present invention, in the key distribution method, each common information generation method includes a first common information generation method, and each shared key obtainment method includes a first shared key obtainment method which is paired with the first common

information generation method. Each of the system secret variable group sets includes first system secret variable groups each of which is made up of one or more first system secret variables. Each of the individual intermediate key group sets includes first individual intermediate key groups each of which is made up of one or more first individual intermediate keys, the first individual intermediate keys are respectively generated based on the first system secret variable groups and one or more first individual intermediate key generation equations. In the key distribution step, one or more time variable generation equations and one or more server shared intermediate key generation equations have been previously provided. In the reception step, one or more receiving device shared intermediate key generation equations have been previously provided. The first common information generation method includes: generating a random number group which is made up of one or more random numbers; generating a time variable group which is made up of one or more time variables based on the random number group, the first system secret variable groups and the time variable generation equations; generating shared intermediate keys based on the first system secret variable groups, the random number group and the server shared intermediate key generation equations; and generating encrypted shared keys by encrypting the shared keys based on the shared intermediate keys. In the first common information generation method of the key distribution method, the key update data includes the time variable group and the encrypted shared keys. The first shared key obtainment method includes: generating the shared intermediate keys based on the time variable group, the first individual intermediate key groups and the receiving device shared intermediate key generation equations; and obtaining the shared keys by decrypting the encrypted shared keys based on the shared intermediate keys.

[0044] In a thirty-third aspect of the present invention, in the

key distribution step of the key distribution method, one of the individual intermediate key group sets has been previously provided, and the key reception step includes storing the previously provided individual intermediate key group set. Each common information
5 generation method includes a first common information generation method, and each shared key obtainment method includes a first shared key obtainment method which is paired with the first common information generation method. Each of the system secret variable group sets includes first system secret variable
10 groups each of which is made up of one or more first system secret variables. Each of the individual intermediate key group sets includes first individual intermediate key groups each of which is made up of one or more first individual intermediate keys, the first individual intermediate keys are respectively generated based on
15 the first system secret variable groups and one or more first individual intermediate key generation equations. The server has been previously provided with one or more time variable generation equations and one or more server shared intermediate key generation equation. Each of the receiving devices has been
20 previously provided with one or more receiving device shared intermediate key generation equations. The first common information generation method includes: generating a random number group which is made up of one or more random numbers; generating a time variable group which is made up of one or more
25 time variables based on the random number group, the first system secret variable groups and the time variable generation equations; generating shared intermediate keys based on the first system secret variable groups, the random number group and the server shared intermediate key generation equations; and generating
30 encrypted shared keys by encrypting the shared keys based on the shared intermediate keys. In the first common information generation method, the key update data includes the time variable

group and the encrypted shared keys. The first shared key
obtainment method includes: generating the shared intermediate
keys based on the time variable group, the first individual
intermediate key group and the receiving device shared
5 intermediate key generation equations; and obtaining the shared
keys by decrypting the encrypted shared keys based on the shared
intermediate keys.

[0045] In the thirty-second aspect of the present invention, in
the key distribution method, each common information generation
10 method includes a second common information generation method,
and each shared key obtainment method includes a second shared
key obtainment method which is paired with the second common
information generation method. Each of the system secret variable
group sets includes a second system secret key group which is made
15 up of second system secret keys. Each of the individual
intermediate key group sets includes second individual intermediate
key groups each of which is made up of one or more of the second
system secret keys. The second common information generation
method includes: generating encrypted shared keys by encrypting
20 the shared keys based on one or more of the second system secret
keys which are included in the second system secret key groups;
and generating an encrypted shared key group which is made up of
the encrypted shared keys combined with each other. In the
second common information generation method of the key
25 distribution system, the key update data includes the encrypted
shared key group. The second shared key obtainment method
includes: selecting one of the encrypted shared keys which
corresponds to any of the second system secret keys included in the
second individual intermediate key group, from among the
30 encrypted shared key group included in the key update data; and
obtaining the shared key by decrypting the selected encrypted
shared key based on the second system secret key.

[0046] In a thirty-fifth aspect of the present invention, the key distribution method, the individual intermediate key group set includes a second individual intermediate key group which is made up of one of the second system secret keys.

5

Effect of Invention

[0047] The key distribution system of the present invention enables to trace the receiving device which is a leakage source by searching an intermediate key which has been embedded in an unauthorized receiving device, even in the case where an attacker obtains the individual key which has been embedded in the receiving device in an unauthorized manner and creates an unauthorized receiving device in which an intermediate key, which can be obtained based on the individual key, is embedded. This is because the intermediate key includes the information indicating the individual key based on which the intermediate key has been generated.

[0048] Also, since the intermediate key has been made to be composed of several individual intermediate keys, even if the individual information of one of the individual intermediate keys is forged, it becomes possible to specify the receiving device which is a leakage source using the rest of the individual intermediate keys. Therefore the traceability is increased resulting in the increase of the reliability.

[0049] The embodiments of the key distribution system concerning the present invention will be described below with reference to figures.

Brief Description of Drawings

[0050] (FIG. 1) A schematic diagram of the key distribution system 1 in a first embodiment of the present invention.

(FIG. 2) A diagram showing an example structure of the key

distribution center 11 in the first embodiment of the present invention.

(FIG. 3) A diagram showing an example structure of the first individual information generation unit 112 in the first embodiment
5 of the present invention.

(FIG. 4) A diagram showing an example structure of the term information storage unit 1122 in the first embodiment of the present invention.

(FIG. 5) A diagram showing an example of the first system secret
10 variable group SPGI_1 in the first embodiment of the present invention.

(FIG. 6) A diagram showing an example of the first individual information EMMI in the first embodiment of the present invention.

(FIG. 7) A diagram showing an example structure of the receiving
15 device information storage unit 113 in the first embodiment of the present invention.

(FIG. 8) A diagram showing an example structure of the second individual information generation unit 114 in the first embodiment of the present invention.

(FIG. 9) A diagram showing an example of the second system
20 secret variable group SPGII in the first embodiment of the present invention.

(FIG. 10) A diagram showing an example of the second individual intermediate key group MKIIGa in the first embodiment of the
25 present invention.

(FIG. 11) A diagram showing an example of the second individual information EMMII in the first embodiment of the present invention.

(FIG. 12) A diagram showing an example of the system secret
30 variable group set SPGS in the first embodiment of the present invention.

(FIG. 13) A diagram showing an example of the individual information group EMMG in the first embodiment of the present

invention.

(FIG. 14) A flow chart of the processing of how the key distribution center 11 distributes the key information in the first embodiment of the present invention.

5 (FIG. 15) A flow chart of the processing of how the key distribution center 11 generates the first system secret variable group SPGI and the first individual information EMMI in the first embodiment of the present invention.

(FIG. 16) A flow chart of the processing of how the key distribution
10 center 11 generates the second system secret variable group SPGII and the second individual information EMMII in the first embodiment of the present invention.

(FIG. 17) A diagram showing an example structure of the server 12 in the first embodiment of the present invention.

15 (FIG. 18) A diagram showing an example structure of the system secret variable group storage unit 122 in the first embodiment of the present invention.

(FIG. 19) A diagram showing an example structure of the first common information generation unit 125 in the first embodiment of
20 the present invention.

(FIG. 20) A diagram showing an example of the time variable group PRG in the first embodiment of the present invention.

(FIG. 21) A diagram showing an example of the first common information ECMI in the first embodiment of the present invention.

25 (FIG. 22) A diagram showing an example structure of the second common information generation unit 126 in the first embodiment of the present invention.

(FIG. 23) A diagram showing an example of the encrypted shared key group ENCSKG in the first embodiment of the present invention.

30 (FIG. 24) A diagram showing an example of the second common information ECMII in the first embodiment of the present invention.

(FIG. 25) A flow chart showing the processing of how the system

secret variable group set SPGS of the server 12 is received in the first embodiment of the present invention.

(FIG. 26) A flow chart of the processing of how the shared keys SK of the server 12 are updated in the first embodiment of the present invention.

(FIG. 27) A diagram showing an example structure of the receiving device 13a in the first embodiment of the present invention.

(FIG. 28) A diagram showing an example structure of the individual key storage unit 1304a in the first embodiment of the present invention.

(FIG. 29) A diagram showing an example of the first encrypted individual intermediate key group set ENCMKIGS in the first embodiment of the present invention.

(FIG. 30) A diagram showing an example of the first individual intermediate key group MKIGa in the first embodiment of the present invention.

(FIG. 31) A diagram showing an example structure of the individual intermediate key storage unit 1305a in the first embodiment of the present invention.

(FIG. 32) A flow chart of how the key distribution center 11 of the receiving device 13a receives the individual information group EMMG in the first embodiment of the present invention.

(FIG. 33) A flow chart indicating the processing of how the common information ECM is received from the server 12 of the receiving device 13a in the first embodiment of the present invention.

(FIG. 34) A schematic diagram of the key distribution system 2 in a second embodiment of the present invention.

(FIG. 35) A diagram showing an example structure of the key distribution center 21 in the second embodiment of the present invention.

(FIG. 36) A diagram showing an example structure of the third

individual information generation unit 212 in the second embodiment of the present invention.

(FIG. 37) A diagram showing an example of the third system secret variable group set SPGIIIS in the second embodiment of the present invention.

(FIG. 38) A diagram showing an example of the third individual information EMMIII in the second embodiment of the present invention.

(FIG. 39) A flow chart indicating the processing of how the key distribution center 21 distributes key information in the second embodiment of the present invention.

(FIG. 40) A flow chart indicating the processing of how the key distribution center 21 generates the third system secret variable group set SPGIIIS and the third individual information EMMIII in the second embodiment of the present invention.

(FIG. 41) A diagram showing an example structure of the server 22 in the second embodiment of the present invention.

(FIG. 42) A diagram showing an example structure of the system secret variable group storage unit 222 in the second embodiment of the present invention.

(FIG. 43) A diagram showing an example of the third common information ECMIII in the second embodiment of the present invention.

(FIG. 44) A flow chart of the processing of how the server 22 receives the third system secret variable group set SPGIIIS in the second embodiment of the present invention.

(FIG. 45) A flow chart indicating the processing of how the server 22 updates the shared keys SK in the second embodiment of the present invention.

(FIG. 46) A diagram showing an example structure of the receiving device 23a in the second embodiment of the present invention.

(FIG. 47) A diagram showing an example structure of the

individual key storage unit 2304a in the second embodiment of the present invention.

(FIG. 48) A diagram showing an example structure of the individual intermediate key storage unit 2305a in the second embodiment of the present invention.

(FIG. 49) A flow chart indicating the processing of how the third individual information group EMMIII is received from the key distribution center 21 of the receiving device 23a in the second embodiment of the present invention.

(FIG. 50) A flow chart indicating the processing of how the third common information ECMIII is received from the server 22 of the receiving device 23a in the second embodiment of the present invention.

(FIG. 51) A variation of the key distribution system 1 in the first embodiment of the present invention.

(FIG. 52) A variation of the first common information generation unit 125 in the first embodiment.

(FIG. 53) A schematic diagram of a conventional key distribution system.

Descriptions of Reference Numerals

[0051] 10 Communication channel

11 and 21 Key distribution center

12 and 22 Server

13a to 13n and 23a to 23n Receiving device

111 and 211 First control unit

112 First individual information generation unit

212 Third individual information generation unit

1121 Term selection unit

2121 Third system secret variable group generation unit

1122 Term information storage unit

2122 First intermediate key group generation unit

1123 Term key encryption unit
 113 Receiving device information storage unit
 114 Second individual information generation unit
 1141 Second system secret key generation unit
 5 1142 Second individual intermediate key group encryption unit
 115 System secret variable group set sending unit
 215 Third system secret variable group set sending unit
 116 Individual information group distribution unit
 216 Third individual information distribution unit
 10 121 and 221 System secret variable group set receiving unit
 122 and 222 System secret variable group storage unit
 123 Shared key generation unit
 124 Common information generation unit selection unit
 125 First common information generation unit
 15 225 Third common information generation unit
 1251 Time variable group generation unit
 1252 Shared intermediate key obtainment unit
 1253 First shared key encryption unit
 1254 Second control unit
 20 126 Second common information generation unit
 1261 Second shared key encryption unit
 1262 Third control unit
 127 and 227 Common information distribution unit
 1301 and 2301 Individual information group receiving unit
 25 1302a First individual intermediate key group obtainment unit
 2302a Third individual intermediate key group obtainment unit
 1303a Second individual intermediate key group obtainment unit
 1304a and 2304a Individual key storage unit
 1305a and 2305a Individual intermediate key storage unit
 30 1306 and 2306a Common information receiving unit
 1307a Shared key obtainment unit selection unit
 1308a First shared key obtainment unit

2308a Third shared key obtainment unit
1309a Second shared key obtainment unit
1310 Output unit

5 **Best Mode for Carrying Out the Invention**

[0052] (First Embodiment)

The key distribution system 1 as an embodiment concerning the present invention will be described. First, the outline of this embodiment will be described with reference to FIG. 1.

10 [0053] In FIG. 1, the communication channel 10 is a communication channel with which the key distribution center 11, the server 12 and the receiving devices 13a to 13n which will be described later are connected, and is realized by means of a network such as the Internet and a broadcasting network. The key
15 distribution center 11 distributes, to the server 12, the system variable group set SPGS which is the information necessary for distributing shared keys SK to receiving devices, and distributes, to the receiving devices 13a to 13n, the individual information group EMMG which is necessary for obtaining the shared keys SK. The
20 server 12 distributes, to the receiving devices 13a to 13n, the common information ECM which has been generated based on the shared keys SK and the system secret variable group set SPGS. The receiving devices 13a to 13n obtain the shared keys SK based on the individual information group EMMG and the common information
25 ECM and outputs the shared keys SK to outside. Here, it is assumed that each pair of the key distribution center 11 and the respective receiving devices 13a to 13n has been provided with an individual key which is previously shared by each pair. For example, it is assumed that the key distribution center 11 and the receiving
30 device 13a previously share an individual key IKa, the key distribution center 11 and the receiving device 13b previously share an individual key IKb, ..., and the key distribution center 11 and the

receiving device 13n previously share an individual key IKn.

[0054] Here, the operation of each component will be described in more detail. First, here will be described a method for distributing, to the respective receiving devices 13a to 13n, the first individual intermediate key groups MKIGa to MKIGn and the second individual intermediate key groups MKIIGa to MKIIGn both of which are respectively different from each other of a kind. First, the key distribution center 11 generates a system secret variable group set SPGS and sends the system secret variable group set SPGS to the server 12. Also, the key distribution center 11 generates an individual information group EMMG which is necessary for the receiving devices to obtain the first individual intermediate key groups and the second individual intermediate key groups, based on the first individual intermediate key groups MKIGa to MKIGn, the second individual intermediate key groups MKIIGa to MKIIGn, and the individual keys Ika to Ikn, and then distributes, to the receiving devices 13a to 13n, the individual keys Ika to Ikn. The receiving device 13a which has received the individual information group EMMG obtains, using the individual key Ika which has been previously provided, the first individual intermediate key group MKIGa and the second individual intermediate key group MKIIGa which are associated with the receiving device 13a. Likewise, the receiving devices 13b to 13n excluding the receiving device 13a obtains, using the individual keys which have been held by the respective receiving devices, the first individual intermediate key groups and the second individual intermediate key groups which are associated with the respective receiving devices. In this way, the respective receiving devices 13a to 13n can hold the first individual intermediate key groups MKIGa to MKIGn and the second individual intermediate key groups MKIIGa to MKIIGn which are respectively different.

[0055] Next, the operation of how the server 12 updates shared

keys SK will be described. First, the server 12 generates one of the first common information ECMI and the second common information ECMII based on the system secret variable group set SPGS according to a previously provided condition, and distributes the generated one, to the receiving devices 13a to 13n, as common information ECM including a common information identifier for identifying one of the first common information ECMI and the second common information ECMII. The receiving devices 13a to 13n receive the common information ECM and determine which one of the first common information ECMI and the second common information ECMII is included in the common information ECM based on the common information identifier included in the common information ECM. In the case where the included one is the first common information ECMI, the server obtains shared keys SK using the first individual intermediate key group and the first common information ECMI. On the other hand, in the case of the second common information ECMII, the server obtains shared keys SK using the second individual intermediate key group and the second common information ECMII. In this way, the shared keys SK of the receiving devices 13a to 13n are updated.

[0056] Note that, in the key distribution system 1 which is this embodiment, it also become possible for the key distribution center 11 to disable the receiving device which has the specific individual key in order to prevent the receiving device from obtaining a shared key SK. This can be realized by not using the individual key which is held by the receiving device to be disabled so that the receiving device to be disabled cannot obtain the first individual intermediate key group and the second individual intermediate key group, in the case where the system secret variable group set SPGS, the first individual intermediate key group and the second individual intermediate key group are updated in the key distribution center 11.

[0057] The outline of this embodiment has been described above. Details of the key distribution system 1 which is an embodiment of the key distribution system of the present invention will be described below. The components of the system will be described
5 in detail.

[0058] <Structure of Key Distribution System 1>

As shown in FIG. 1, the key distribution system 1 includes: a communication channel 10; a key distribution center 11; a server 12; and receiving devices 13a to 13n.

[0059] The key distribution center 11 distributes, to the server 12, a system secret variable group set SPGS which is the information necessary for distributing the shared keys SK to the receiving devices 13a to 13n, and distributes, to the receiving devices 13a to 13n, the individual information group EMMG which is necessary for
10 receiving the shared keys SK from the server 12. The server 12 generates shared keys SK, generates common information ECM based on the shared keys SK and the system secret variable group set SPGS, and distributes the common information ECM to the receiving devices 13a to 13n. The receiving devices 13a to 13n
15 obtain the shared keys SK based on the individual information group EMMG and the common information ECM, and output them to outside.

[0060] The components will be described below in detail. First, the structure of the communication channel 10 will be described, and consequently the structures and the operations of the key
20 distribution center 11, the server 12 and the receiving devices 13a to 13n will be described with reference to figures.

[0061] <Structure of Communication Channel 10>

The communication channel is a network such as the Internet, a telephone circuit, an exclusive line and a broadcasting network.
25

[0062] <Structure of Key Distribution Center 11>

As shown in FIG. 2, the key distribution center 11 includes: a

first control unit 111; a first individual information generation unit 112; a receiving device information storage unit 113; a second individual information generation unit 114; a system secret variable group set sending unit 115; and an individual information group distribution unit 116.

[0063] (1) First Control unit 111

In the case where an individual information update condition which has been previously provided is satisfied, or in the case where the key distribution center 13 starts its operation, the first control unit 111 outputs the first individual information generation request REQEMMI to the first individual information generation unit 112, and outputs the second individual information generation request REQEMMII to the second individual information generation unit 114. Example individual information update conditions include "every a certain time period (example: everyday; and every year)" and "in the case where a signal has been received from outside.". In the case where the individual information update condition is "every a certain time period (example: everyday; and every year)", the counter can be updated by means that the first control unit 111 includes a counter. In the case where the individual information update condition is "in the case where a signal has been received from outside", the counter can be updated by means that the first control unit 111 includes a receiving unit which receives a signal from outside.

[0064] (2) First Individual Information Generation Unit 112

As shown in FIG. 3, the first individual information generation unit 112 includes: a term selection unit 1121; a term information storage unit 1122; and a term key encryption unit 1123.

[0065] (2-1) Term Selection Unit 1121

In the case where the term selection unit 1121 receives the first individual information generation request REQEMMI from the first control unit 111, it accesses the term information storage unit

1122. The term information storage unit 1122 stores k numbers of sets of: an unused flag (one of FLAG_1 to FLAG_k); a term identifier (one of PID_1 to PID_k); a term key (one of PK_1 to PK_k); and first system secret variable group (one of SPGI_1 to SPGI_k), the sets being {(FLAG_1, PID_1, PK_1, SPGI_1), (FLAG_2, PID_2, PK_2, SPGI_2),..., (FLAG_k, PID_k, PK_k, SPGI_k)}. After that it selects a set having an unused flag bit of "1" from among the k numbers of sets. Also, it resets the unused flag bit 1 of the selected set at "0". As an example method for selecting a set having an unused flag bit of "1" from among the k numbers of sets having an unused flag bit of "1", there is a method for selecting a set at random using a random number. As to the method for generating a random number, Non-patent Reference 3 is detailed. It is assumed that the respective values of the sets selected by the term selection unit 1121 are hereinafter referred to as unused flag FLAG_i, a term identifier PID_i, a term key PK_i, and a first system secret variable group SPGI. Here, an unused flag FLAG_i is one of the unused flags FLAG_1 to FLAG_k, a term identifier PID_i is one of the term identifier PID_1 to PID_k, a term key PK_i is one of the term keys PK_1 to PK_k, and a first system secret variable group SPGI_i is one of the first system secret variable group SPGI_1 to SPGI_k. Next, it outputs the selected first system secret variable group SPGI_i to the system secret variable group set sending unit 115 as a first system secret variable group SPGI. After that, lastly, it outputs the selected term identifier PID_i and the term key PK_i to the term key encryption unit 1123.

[0066] (2-2) Term Information Storage Unit 1122

As shown in FIG. 4, the term information storage unit 1122 stores k numbers of prepared sets of: an unused flag; a term identifier; a term key; and a first system secret variable group, the sets being {(FLAG_1, PID_1, PK_1, SPGI_1), (FLAG_2, PID_2, PK_2, SPGI_2),..., (FLAG_k, PID_k, PK_k, SPGI_k)}. For example, FIG. 4

shows the statuses where: (a) the term key PK₁, the first system secret variable group SPGI₁ and an unused flag FLAG₁ are held in association with the term identifier PID₁; (b) the term key PK₂, the first system secret variable group SPGI₂ and an unused flag FLAG₂ are held in association with the term identifier PID₂; and (c) the term key PK_k, the first system secret variable group SPGI_k and an unused flag FLAG_k are held in association with the term identifier PID_k. Here, as shown in FIG. 5, the first system secret variable group SPGI₁ is composed of five first system secret variables (s₁, t₁, u₁, v₁, and c₁). Also, the other first system secret variable groups SPGI₂ to SPGI_k are respectively composed of: s₂, t₂, u₂, v₂, and c₂; and s_k, t_k, u_k, v_k, and c_k. Further, it is assumed that the first system secret variables have been provided so that the following first system secret variable generation equations are satisfied: "s₁*t₁=u₁*v₁ mod N"; "s₂*t₂=u₂*v₂ mod N"; and "s_k*t_k=u_k*v_k mod N". For example, the five first system secret variables and the moduluses N are natural numbers of, for example, 128 bits. The values of these moduluses N here are the same values as these moduluses N which have been previously provided as shared values to the later-described time variable group generation unit 1251, shared intermediate key obtainment unit 1252 and first shared key obtainment unit 1308a, and an example value is 2^{128}. Also, "mod N" is a remainder operation, and "^" represents a power operation. For example, 2^{4} means 16 and they both are used in the same meaning hereinafter. Note that the following method is available as a generation method of a first system secret variable group (example: SPGI₁): the method of generating four first system secret variables (example: s₁, t₁, u₁ and c₁) as random numbers; substituting three first system secret variables (example: s₁, t₁, and u₁) among the four first system secret variables to the first system secret variable

generation equation " $s_1 \cdot t_1 = u_1 \cdot v_1 \bmod N$ "; and obtaining the remaining one of the first system secret variables (example: v_1). Also, the respective unused flags FLAG_1 to FLAG_k are made up of "0" or "1", and they are, for example, natural numbers. Note that it is assumed that all the unused flags FLAG_1 to FLAG_k are "1" in the case where the key distribution center 11 starts its operation. Also, the receiving device identifiers AIDa to AIDn are the identifiers which are uniquely associated with the receiving devices 13a to 13n, and they are, for example, natural numbers. Further, the respective term keys PK_1 to PK_k are keys in the DES encryption method which are described in, for example, the Non-patent Reference 2, and they are generated using random numbers or the like. Also, the term identifiers PID_1 to PID_k take respectively different numbers, and they are, for example, respectively different natural numbers.

[0067] (2-3) Term Key Encryption Unit 1123

In the case where the term key encryption unit 1123 receives a term identifier PID_i and a term key PK_i from the first system variable group selection unit, it accesses the receiving device information storage unit 114 and obtains all the receiving device identifiers AIDa to AIDn and individual keys IKa to Ikn. After that, firstly, it encrypts the term key PK_i based on the individual key IKa which corresponds to the receiving device identifier AIDa, considers the encrypted sentence as an encrypted term key $ENCPKa = \text{Enc}(IKa, PK_i)$, and associates it with the receiving device identifier AIDa. After that it encrypts the remaining terminal keys based on the individual keys which correspond to the other receiving device identifiers AIDb to AIDn as well, considers the encrypted sentences $\text{Enc}(IKb, PK_i), \dots, \text{Enc}(Ikn, PK_i)$ as an encrypted term keys $ENCPKb, \dots, ENCPKn$, and then associates them with the respective receiving device identifiers AIDb to AIDn. After that, it generates a first individual information, shown in FIG. 6, which is composed of:

a term identifier PID_i ; one of the device identifiers $AIDa$ to $AIDn$; and one of the encrypted term keys $ENCPKa$ to $ENCPKn$, and outputs the first individual information EMMI to the individual information group distribution unit 116, the first individual information EMMI equals to $PID_i || \{AIDa, ENCPKa\} || \{AIDb, ENCPKb\}, \dots || \{AIDn, ENCPKn\}$. Here, the encryption algorism which is used for encrypting the terminal keys is, for example, the DES encryption method which is described in the Non-patent Reference 2, and the method to be used is the same as the method of the decryption algorism which is used at the time of decrypting the encrypted term keys in the individual intermediate group obtainment unit 1302a of the later-described receiving devices 13a to 13n.

[0068] (3) Receiving Device Information Storage Unit 113

As shown in FIG. 7, the receiving device information storage unit 113 stores: the receiving device identifiers $AIDa$ to $AIDn$ for identifying the receiving devices 13a to 13n; and the individual keys IKa to IKn which have been previously provided to the respective receiving devices 13a to 13n. For example, FIG. 7 shows the statuses where: the receiving device 13a which is associated with the receiving device identifier $AIDa$ holds the individual key IKa ; the receiving device 13b which is associated with the receiving device identifier $AIDb$ holds the individual key IKb ; and the receiving device 13n which is associated with the receiving device identifier $AIDn$ holds the individual key IKn . It is possible to access the receiving device information storage unit 113 through the term key encryption unit 1123 of the first individual information generation unit 112 and the second individual intermediate key group encryption unit 1142 of the second individual information generation unit 114.

[0069] (4) Second Individual Information Generation Unit 114

As shown in FIG. 8, the second individual information generation unit 114 is composed of the second system secret key generation unit 1141 and the second individual intermediate key

group encryption unit 1142.

[0070] (4-1) Second System Secret Key Generation Unit 1141

In the case where the second system secret key generation unit 1141 receives the second individual information generation request REQEMMII from the first control unit 111, it generates six second system secret keys k1, k2, k3, k4, k5 and k6. As example method for generating six second system secret keys k1, k2, k3, k4, k5 and k6, there is a method of generating them at random. More concretely, they can be realized using, for example, random numbers. The Non-patent Reference 3 describes a method for generating random numbers in detail. After that, it generates second system secret variable group SPGII which is composed of six second system secret keys k1, k2, k3, k4, k5 and k6 shown in FIG. 9, and outputs them to the system secret variable group set sending unit 115 and the second individual intermediate key group encryption unit 1142.

[0071] (4-2) Second Individual Intermediate Encryption Unit 1142

In the case where the second individual intermediate key group encryption unit 1142 receives a second system secret variable group SPGII from the second system secret key generation unit 1141, it accesses the receiving device information storage unit 113, and obtains all the receiving device identifiers AIDa to AIDn and individual keys IKa to IKn. After that, firstly, it selects a second secret key from among the six second system secret keys k1, k2, k3, k4, k5 and k6 which are included in the second system secret variable group SPGII in association with the receiving device identifier AIDa. As an example method for selecting a second system secret key, there is a method of selecting one at random, and it can be realized using a random number. Here, as an example, it is assumed that the key which has been selected in association with the receiving device identifier AIDa is the second system secret key

k1. In this case, as shown in FIG. 10, the second individual intermediate key group MKIIGa becomes the second system secret key k1. After that, it encrypts the second individual intermediate key group MKIIGa based on the corresponding individual key IKa, considers the encrypted sentence as the encrypted second individual intermediate key group ENCMKIIGa=Enc(IKa, MKIIGa), and then associates it with the receiving device identifier AIDa. After that, it selects a second system secret key from among the six second system secret keys in the second system secret variable group SPGII which corresponds to the other receiving device identifiers AIDb to AIDn as well, considers the second system secret key as the second individual intermediate key group, encrypts the second individual intermediate key group based on the corresponding individual key, considers the encrypted sentence Enc(IKb, MKIIGb),..., Enc(IKn, MKIIGn) as the second encrypted individual intermediate key group ENCMKIIGb,..., ENCMKIIGn, and then associates them with the respective receiving device identifiers AIDb to AIDn. After that, it generates the second individual information EMMII which is composed of: the receiving device identifiers AIDa to AIDn; and the second encrypted individual intermediate key groups ENCMKIIGa to ENCMKIIGn, the second individual information EMMII equals to AIDa, ENCMKIIGa}{AIDb, ENCMKIIGb},...{AIDn, ENCMKIIGn}}, and outputs the second individual information EMMII to the individual information group distribution unit 116. An encryption algorism which is used for encrypting the second individual intermediate key group here is, for example, a DES encryption method which is described in the Non-patent Reference 2, and the method used here is the same as the method of the decryption algorism which is used at the time of decrypting the second encrypted individual intermediate key group in the second individual intermediate group obtainment unit 1303a of the later-described receiving devices 13a to 13n.

[0072] (5) System Secret Variable Group Set Sending Unit 115

In the case where the system secret variable group set sending unit 115 receives the first system secret variable group SPGI from the first system secret variable group selection unit 1121 of the first individual information generation unit 112, and also receives the second system secret variable group SPGII from the second system secret key generation unit 1141 of the second individual information generation unit 114, it generates a system secret variable group set SPGS, shown in FIG. 12, which is composed of: the first system secret variable group SPGI and the corresponding system secret variable group identifier SPGIDI; and the second system secret variable group SPGII and the corresponding system secret variable group identifier SPGIDII. After that, the system secret variable group set SPGS is sent to the server 12. Here, the system secret variable group identifier SPGIDI and the system secret variable group identifier SPGIDII are, for example, natural numbers. Note that the system secret variable group identifier SPGIDI and the system secret variable group identifier SPGIDII are used in order to differentiate the first system secret variable group SPGI from the second system secret variable group SPGII. However, in the case where the key distribution center 11 and the server 12 previously share the information such as bit positions of the first system secret variable group SPGI and the second system secret variable group SPGII in the communication data, the system secret variable group set SPGS does not need to always include a system secret variable group identifier SPGIDI and a system secret variable group identifier SPGIDII.

[0073] (6) Individual Information Group Distribution Unit 116

In the case where the individual information group distribution unit 116 receives the first individual information EMMI from the term key encryption unit 1123 of the first individual

information generation unit 112 and receives the second individual information EMMII from the second individual intermediate key group encryption unit 1142 of the second individual information generation unit 114, it generates, as shown in FIG. 13, the individual information group EMMG which is composed of: the first individual information EMMI and the corresponding individual information identifier EMMIDI; and the second individual information EMMII and the corresponding individual information identifier EMMIDII. After that, it distributes the individual information group EMMG to the receiving devices 13a to 13n. Here, the individual identifier EMMIDI and the individual information identifier EMMIDII are, for example, respectively different natural numbers. Note that the individual identifier EMMIDI and the individual information identifier EMMIDII are used for differentiating the first individual information EMMI from the second individual information EMMII. However, in the case where the key distribution center 11 and the receiving devices 13a to 13n previously share the information such as bit positions of the first individual information EMMI and the second individual information EMMII in the communication data, the individual information group EMMG does not need to always include the individual information identifier EMMIDI and the individual information identifier EMMIDII.

[0074] <Operation of Key Distribution Center 11>

The structure of the key distribution center 11 has been described up to this point. Here, the operation of the key distribution center 11 will be described. Here will be described, with reference to the flow chart shown as FIG. 14, how the key distribution center 11 operates at the time of distributing shared keys, and distributing the key information which is necessary for distributing and receiving the shared keys to the server 12 and the receiving devices 13a to 13n, in the case where a previously provided individual information update condition is satisfied, or in

the case where the key distribution center 11 starts its operation or another case. Also, how the first individual information generation unit 112 operates at the time of generating the first system secret variable group SPGI and the first individual information EMMI will be described in detail with reference to the flow chart shown as FIG. 15. Lastly, how the second individual information generation unit 114 operates at the time of generating the second system secret variable group SPGII and the second individual information EMMII will be described in detail with reference to the flow chart shown as FIG. 16.

[0075] <Operation of Key Distribution Center 11 in Distributing Key Information>

The first control unit 111 outputs the first individual information generation request REQEMMI to the first individual information generation unit 112, and outputs the second individual information generation request REQEMMII to the second individual information generation unit 114 (S1101).

According to the flow chart shown as FIG. 15 (details will be described below), the first individual information generation unit 112 generates the first system secret variable group SPGI and the first individual information EMMI, outputs the first system secret variable group SPGI to the system secret variable group set sending unit 115, and outputs the first individual information EMMI to the individual information group distribution unit 116 (S1102).

According to the flow chart shown as FIG. 16 (details will be described below), the second individual information generation unit 114 generates the second system secret variable group SPGII and the second individual information EMMII, outputs the second system secret variable group SPGII to the system secret variable group set sending unit 115, and outputs the second individual information EMMII" to the individual information group distribution unit 116 (S1103).

The system secret variable group set sending unit 115 which

has received the first system secret variable group SPGI and the second system secret variable group SPGII, generates a system secret variable group set SPGS which is composed of the first system secret variable group SPGI and the second system secret variable group SPGII, and sends the system secret variable group set SPGS to the server 12 (S1104).

The individual group distribution unit 116 which has received the first individual information EMMI and the second individual information EMMII, generates an individual information group EMMG which is composed of the first individual information EMMI and the second individual information EMMII, distributes the individual information group EMMG to the receiving devices 13a to 13n to complete the operation (S1105).

<Operation of Key Distribution Center 11 in Generating First System Secret Variable Group SPGI and First Individual Information EMMI (Detailed Description of Step 1102)>

The first system secret variable group selection unit 1121, which has received the first individual information generation request REQEMMI, accesses the term information storage unit 1122, and obtains a set which is associated with an unused flag bit of "1" and made up of a term identifier (example: PID_i), a term key (example: PK_i) and a first system secret variable group (example: SPGI_i). After that, it resets the unused flag (example: FLAG_i) which is stored in the term selection unit 1121 as "0" (S11021).

The first system secret variable group selection unit 1121 outputs a first system secret variable group (example: SPG1_i) to the system secret variable group set sending unit 115 as the first system secret variable group SPG1 (S11022).

The first system secret variable group selection unit 1121 outputs a term identifier (example: PID_i) and a term key (example: PK_i) to the term key encryption unit 1123 (S11023).

The term key encryption unit 1123, which has received the

term identifier (example: PID_i) and the term key (example: PK_i), accesses the receiving device information storage unit 114, and obtains all the sets of the receiving device identifiers AIDa to AIDn and individual keys IKa to IKn (S11024).

5 The term key encryption unit 1123 encrypts the term key (example: PK_i) based on the respective individual keys IKa to IKn, and generates the encrypted term keys (examples: ENCPKa=Enc(IKa, PK_i),...,ENCPKn=Enc(IKn, IKn))(S11025).

10 It respectively associates the encrypted term keys ENCPKa to ENCPKn with the receiving device identifiers AIDa to AIDn corresponding to the individual keys which have been used at the time of the encryption of the encrypted term keys, and further adds a term identifier (example: PID_i) to them so as to generate the first individual information EMMI (example: the first individual
15 information=PID_i||{AIDa, ENCPKa}||{AIDb, ENCPKb},...,{AIDn, ENCPKn}) (S11026).

 The term key encryption unit 1123 outputs the first individual information EMMI to the individual information group distribution unit 116 to complete the operation (S11027).

20 <Operation of Key Distribution Center 11 in Generating Second System Secret Variable Group SPGII and Second Individual Information EMMII (Detailed Description of Step 1103)>

 The second system secret key generation unit 1141, which has received the second individual information generation request
25 REQEMMII, generates six second system secret keys k1,k2, k3, k4, k5 and k6 (S11031).

 The second system secret key generation unit 1141 generates a second system secret variable group SPGII which is composed of six second system secret keys k1, k2, k3, k4 k5 and k6 (S11032).

30 The second system secret key generation unit 1141 outputs the second system secret variable group SPGII to the system secret variable group set sending unit 115 and the second individual

intermediate key group encryption unit 1142 (S11033).

The second individual intermediate key group encryption unit 1142, which has received the second system secret variable group SPGII, accesses the receiving device information storage unit 113, and obtains all the receiving device identifiers AIDa to AIDn and individual keys IKa to Ikn (S11034).

The second individual intermediate key group encryption unit 1142 selects a second system secret key (example: MKIIGa=k1, MKIIGb=k2,...,MKIIGn=k6) from among the second system secret variable groups SPGII in association with the respective receiving device identifiers AIDa to AIDn, and considers them as the second individual intermediate key groups MKIIGa to MKIIGn (S11035).

The second individual intermediate key group encryption unit 1142 encrypts the respective second individual intermediate key groups MKIIGa to MKIIGn based on the individual key IKa, and considers the encrypted sentence as the second encrypted individual intermediate key group ENCMKIIGa=Enc(IKa, MKIIGa), ENCMKIIGb=Enc(IKb, MKIIGb),..., ENCMKIIGn=Enc(IKn, MKIIGn) (S11036).

The second individual intermediate key group encryption unit 1142 generates a second individual information EMMII={AIDa, ENCMKIIGa}||{AIDb, ENCMKIIGb},...,||{AIDn, ENCMKIIGn} which is composed of the receiving device identifiers AIDa to AIDn and the second encrypted individual intermediate key groups ENCMKIIGa to ENCMKIIGn (S11037).

[0076] The second individual intermediate key group encryption unit 1142 outputs the second individual information EMMII to the individual information group distribution unit 116 (S11038).

The structure and the operation of the key distribution center 11 which is a component of the key distribution system 11 have been described up to this point, and the structure and the operation of the server 12 will be described next.

[0077] <Structure of Server 12>

As shown in FIG. 17, the server 12 includes: a system secret variable group set receiving unit 121; a system secret variable group storage unit 122; a shared key generation unit 123; a common information generation unit selection unit 124; a first common information generation unit 125; a second common information generation unit 126; and a common information distribution unit 17.

[0078] (1) System Secret Variable Group Set Receiving Unit 121

In the case where the system secret variable group set receiving unit 121 receives a system secret variable group set SPGS from the key distribution center 11, it extracts the first system secret variable group SPGI and the second system secret variable group SPGII based on the SPGIDI and the SPGIDII which are the system secret variable group identifiers included in the received system secret variable group set SPGS, stores the system secret variable group storage unit 122 like shown in FIG. 18, and outputs the shared key generation request REQSK to the shared key generation unit 123.

[0079] (2) System Secret Variable Group Storage Unit 122

As shown in FIG. 18, the system secret variable group storage unit 122 is for storing a first system secret variable group SPGI and a second system secret variable group SPGII. It is possible to access the system secret variable group storage unit 122 from: the system secret variable group set receiving unit 121 and the time variable group generation unit 1251 in the first common information generation unit 125; and the shared intermediate key obtainment unit 1252 and the second shared key encryption unit 1261 in the second common information generation unit 126.

[0080] (3) Shared Key Generation Unit 123

In the case where the shared key generation unit 123 receives the shared key generation request REQSK from the system secret

variable group set receiving unit 121, or in the case where a previously provided common information update condition is satisfied, a shared key SK is generated. As an example method for generating a shared key SK, there is a method of generating a shared key SK at random using a random number. The Non-patent Reference 3 describes in detail the method of generating a random number. After that, the shared key SK is outputted to the common information generation unit selection unit 124. For example, in the case where the common information update condition is "every second", "every hour" or the like, a counter can be updated by means that the shared key generation unit 123 has the counter, and in the case where the common information update condition is "in the case where a specific signal has been received from outside" or the like, a counter can be updated by means that the shared key generation unit 123 has a receiving unit which receives a signal from outside.

[0081] (4) Common information Generation Unit Selection Unit 124

In the case where the common information generation unit selection unit 124 receives a shared key SK from the shared key generation unit 123, it selects one of the first common information generation unit 125 and the second common information generation unit 126, and outputs the shared key SK to: the selected time variable group generation unit 1251 of the first common information generation unit 125 and the first shared key encryption unit 1253; or the second shared key encryption unit 1261 of the second common information generation unit 126. Here, as a method for selecting one of the first common information generation unit 125 and the second common information generation unit 126, there are a method of selecting one based on the schedule data which is provided from outside and another method of selecting one at random using a random number.

(5) First Common information Generation Unit 125

As shown in FIG. 19, the first common information generation unit 125 includes: a time variable group generation unit 1251; a shared intermediate key obtainment unit 1152; a first shared key encryption unit 1253; and a second control unit 1254.

[0082] (5-1) Time Variable Group Generation Unit 1251

In the case where the time variable group generation unit 1251 receives a shared key SK from the common information generation unit selection unit 124, it generates four random numbers z , w , m and n . Here, as an example method for generating the random numbers z , w , m and n , there is a method of generating them at random using random numbers. Also, the random numbers z , w , m and n are, for example, natural numbers of 128 bits. Also, it accesses the system secret variable group storage unit 122, obtains the first system secret variable group SPGI, and extracts the first system secret variables s , t , u and v from among the first system secret variable group SPGI. After that, it generates four time variables r_1 , r_2 , r_3 and r_4 based on the previously provided four time variable generation equations: " $r_1 = s * z + v * m \bmod N$ "; " $r_2 = t * w + u * n \bmod N$ "; " $r_3 = u * z + t * m \bmod N$ "; and " $r_4 = v * w + s * n \bmod N$ ". After that, it generates a time variable group PRG, like shown in FIG. 20, which is composed of the generated time variables r_1 , r_2 , r_3 and r_4 , and outputs the time variable group PRG to the second control unit 1254. Lastly, it outputs the random numbers z , w , m and n to the shared intermediate key obtainment unit 1252.

[0083] (5-2) Shared Intermediate Key Obtainment Unit 1252

In the case where the shared intermediate key obtainment unit 1252 receives the random numbers z , w , m and n from the time variable group generation unit 1251, it accesses the system secret variable group storage unit 122 first, obtains the first system secret variable group SPGI, and extracts the first system secret variables s , t , u , v and c from the first system secret variable group SPGI. After

that, it generates a shared intermediate key SMK based on the previously provided server shared intermediate key generation equation " $SMK = 2 * s * t * (z + w + c + n * m) + 2 * (u * s * n * z + t * v * m * w) \bmod N$ ", and outputs the generated shared intermediate key SMK to the first shared key encryption unit 1253.

[0084] (5-3) First Shared Key Encryption Unit 1253

In the case where the first shared key encryption unit 1253 receives a shared key SK from the second control unit 124, and further receives the shared intermediate key SMK from the shared intermediate key obtainment unit 1252, it encrypts the received shared key SK based on the shared intermediate key SMK. Here, an encryption algorithm which is used for encrypting the shared key SK is, for example, a DES encryption method, and the method used here is the same as the method of the decryption algorithm which is used for decrypting the encrypted shared key ENCSK in the respective first shared key obtainment units 1308a of the later-described receiving devices 13a to 13n. After that, it outputs the encrypted shared key ENCSK to the second control unit 1254.

[0085] (5-4) Second Control Unit 1254

In the case where the second control unit 1254 receives a time variable group PRG from the time variable group generation unit 1251, and also receives an encrypted shared key ENCSK from the first shared key encryption unit 1253, it generates the first common information ECMI which is composed of: a common information identifier ECMIDI indicating the first common information ECMI; a time variable group PRG; and an encrypted shared key ENCSK, as shown in FIG. 21. After that, it outputs the first common information ECMI to the common information distribution unit 127 as common information ECM. Here, the common information identifier ECMIDI is, for example, a natural number. Note that the common information identifier ECMIDI is used at the time of identifying which one of the following is included

in the common information ECM: the first common information ECMI and the first common information ECMII. However, in the case where the server 12 and the receiving devices 13a to 13n previously share the timing of sending the first common information ECMI and the second common information ECMII, the common information ECM does not need to always include the first common information identifier ECMID1 and the second common information identifier ECMIDII. Such a case is, for example, the case where the server 12 and the receiving devices 13a to 13n send the first common information ECMI at a certain time point, and send the second common information ECMII at the other time points.

[0086] (6) Second Common information Generation Unit 126

As shown in FIG. 22, the second common information generation unit 126 includes: a second shared key encryption unit 1261; and a third control unit 1262.

[0087] (6-1) Second Shared Key Encryption Unit 1261

In the case where the second shared key encryption unit 1261 receives a shared key SK from the second control unit 124, it accesses the system secret variable group storage unit 122 first, obtains the second system secret variable group SPGII, and extracts the second system secret keys k1, k2, k3, k4, k5 and k6 from among the second system secret variable group SPGII. After that, it encrypts the shared key SK based on the second system secret key k1 first, and generates the encrypted shared key ENCSK1=Enc(k1, SK). After that, it encrypts the shared keys SK based on the other second system secret keys k2, k3, k4, k5 and k6 as well, and generates the encrypted shared keys ENCSK2=Enc(k2, SK),..., ENCSK6=Enc(k6, SK). Lastly, it outputs an encrypted shared key group ENCSKG like shown in FIG. 23 to the third control unit 1262, the encrypted shared key group ENCSKG being obtained by combining the encrypted shared keys ENCSK1, ENCSK2, ENCSK3, ENCSK4, ENCSK5, and ENCSK6. Note that an encryption algorithm

which is used here for encrypting the shared keys SK are, for example, a DES encryption method, and the method used here is the same as the method of the decryption algorithm which is used by the respective second shared key obtainment units 1309 of the
5 later-described receiving devices 13a to 13n in order to decrypt one of the encrypted sentences in the encrypted shared key group ENCSKG.

[0088] (6-2) Third Control Unit 1262

In the case where the third control unit 1262 receives an
10 encrypted shared key ENCSKG from the second shared key encryption unit 1261, it generates, as shown in FIG. 24, the second common information ECMII which is composed of the common information identifier ECMIDII indicating the second common information ECMII and the encrypted shared key group ENCSKG.
15 After that, it outputs the second common information ECMII to the common information distribution unit 127 as common information ECM. Here, the common information identifier ECMIDII is, for example, a natural number which is different from the common information identifier ECMIDI. Note that the common information
20 identifier ECMIDII is used at the time of identifying the first common information ECMI or the first common information ECMII that is included in the common information ECM. However, in the case where the server 12 and the receiving devices 13a to 13n previously share the timing of sending the first common information ECMI and
25 the second common information ECMII, the common information ECM does not need to always include the first common information identifier ECMIDI and the second common information identifier ECMIDII. Such a case is, for example, the case where the server 12 and the receiving devices 13a to 13n send the first common
30 information ECMI at a certain time point, and send the second common information ECMII at the other time points.

[0089] (7) Common information Distribution Unit 127

In the case where the common information distribution unit 127 receives common information ECM from one of the second control unit 1254 of the first common information generation unit 125 and the third control unit 1262 of the second common information generation unit 126, it distributes the common information ECM to the receiving devices 13a to 13n.

[0090] <Operation of Server 12>

The structure of the server 12 has been described up to this point. Here, the operation of the server 12 will be described. First, how the server 12 receives, from the key distribution center 11, a system secret variable group set SPGS which is used at the time of distributing a shared key SK will be described with reference to the flow chart shown as FIG. 25. Next, how the server 12 distributes a new shared key SK to the receiving devices 13a to 13n in the case where it receives a shared key generation request REQSK from the system secret variable group set receiving unit 121, or in the case where a previously provided shared key update condition is satisfied will be described with reference to the flow chart shown as FIG. 26.

[0091] <Operation of Server 12 in Receiving System Variable Group Set SPGS from Key Distribution Center 11>

The system secret variable group set receiving unit 121 extracts the first system secret variable group SPGI and the second system secret variable group SPGII based on the system secret variable group identifiers SPGIDI to SPGIDII which are included in the received system secret variable group set SPGS (S1201).

The system secret variable group set receiving unit 121 stores the first system secret variable group SPGI and the second system secret variable group SPGII in the system secret variable group storage unit 122 to complete the operation (S1202).

< Operation of Server 12 in Distributing New Shared Key SK to Receiving Devices 13a to 13n>

The shared key generation unit 123 generates a shared key

SK and outputs it to the common information generation unit selection unit 124 (S1251).

The common information generation unit selection unit 124 selects one of the first common information generation unit 125 and the second common information generation unit 126, and outputs the shared key SK to the selected one. Here, in the case where the first common information generation unit 125 is selected, Step 1254 is executed next. In contrast, in the case where the second common information generation unit 126 is selected, Step 1260 is executed next (S1252).

The first common information generation unit 125, which has received the shared key SK from the shared key information selection unit 124, generates random numbers z , w , m and n . After that, it accesses the system secret variable group storage 122, obtains the first system secret variable group SPGI and extracts the first system secret variables s , t , u and v from the first system secret variable group SPGI. After that, it generates four time variables r_1 , r_2 , r_3 and r_4 based on the previously provided four time variable generation equations: " $r_1 = s \cdot z + v \cdot m \bmod N$ "; " $r_2 = t \cdot w + u \cdot n \bmod N$ "; " $r_3 = u \cdot z + t \cdot m \bmod N$ "; and " $r_4 = v \cdot w + s \cdot n \bmod N$ ". It generates a time variable group PRG which is composed of the generated four time variables r_1 , r_2 , r_3 and r_4 (S1253).

It outputs the time variable group PRG to the second control unit 1254 (S1254).

It outputs the random numbers z , w , m and n to the shared intermediate key obtainment unit 1252 (S1255).

In the case where the shared intermediate key obtainment unit 1252 receives random numbers z , w , m and n from the time variable group generation unit 1251, it accesses the system secret variable group storage unit 122 first, obtains the first system secret variable group SPGI, and extracts the first system secret variables s , t , u , v and c from the first system secret variable group SPGI. After

that, it obtains a shared intermediate key SMK based on the previously provided server shared intermediate key generation equation " $SMK=2*s*t*(z+w+c+n*m)+2*(u*s*n*z+t*v*m*w) \bmod N$ " (S1256).

5 It outputs the generated shared intermediate key SMK to the first shared key encryption unit 1253 (S1257).

 In the case where the first shared key encryption unit 1253 receives a shared key SK from the second control unit 124, and further receives the shared intermediate key SMK from the shared
10 intermediate key obtainment unit 1252, it encrypts the received shared key SK based on the shared intermediate key SMK, and outputs the encrypted shared key ENCSK to the second control unit 1254 (S1258).

 In the case where the second control unit 1254 receives a
15 time variable group PRG from the time variable group generation unit 1251, and also receives the encrypted shared key ENCSK from the first shared key encryption unit 1253, it generates the first common information ECMI which is composed of: a common information identifier ECMIDI indicating the first common
20 information ECMI; a time variable group PRG; and an encrypted shared key ENCSK, outputs the first common information ECMI to the common information distribution unit 127 as common information ECM, and then goes to Step 126 (S1259).

 In the case where the second shared key encryption unit 1261
25 receives a shared key SK from the second control unit 124, it accesses the system variable group storage unit 122 first, obtains the second system secret variable group SPGII and extracts six second system secret keys k1, k2, k3, k4, k5 and k6 from the second system secret variable group SPGII (S1260).

30 The shared key encryption unit 1261 encrypts a shared key SK based on the respective second system secret keys k1, k2, k3, k4, k5 and k6 to generate the encrypted shared keys $ENCSK1=Enc(k1,$

SK), ENCSK2=Enc(k2, SK),..., ENCSK6=Enc(k6, SK), and combines these encrypted shared keys ENCSK1 to ENCSK6 to generate an encrypted shared key group ENCSKG (S1261).

The second shared key encryption unit 1261 outputs the encrypted shared key group ENCSKG to the third control unit 1262 (S1262).

In the case where the third control unit 1262 receives the encrypted shared key group ENCSKG from the second shared key encryption unit 1261, it generates second common information ECMII which is composed of: a common information identifier ECMIDII indicating the second common information ECMII; and an encrypted shared key group ENCSKG, and outputs the second common information ECMII to the common information distribution unit 127 as common information ECM (S1263).

The common information distribution unit 127, which has received the common information ECM, distributes the common information ECM to the receiving devices 13a to 13n to complete the operation (S1264).

The structure and the operation of the server 12 which is a component of the key distribution system 1 have been described up to this point. First, the structure and the operation of the receiving device 13a will be described first, and then the difference between the receiving device 13a and the other receiving devices 13b to 13n will be described.

[0092] <Structure of Receiving Device 13a>

As shown in FIG. 27, the receiving device 13a includes: an individual information receiving unit 1301; a first individual intermediate key group obtainment unit 1302a; a second individual intermediate key group obtainment unit 1303a; an individual key storage unit 1304a; an individual key storage unit 1305a; a common information receiving unit 1306; a second selection unit 1307a; a first shared key obtainment unit 1308a; a second shared key

obtainment unit 1309a; and an output unit 1310. Here, the components which are unique to the receiving device 13a include: the first individual intermediate key group obtainment unit 1302a; the first individual intermediate key group obtainment unit 1303a; the individual key storage unit 1304a; the individual intermediate key storage unit 1305a; the second selection unit 1307a; the first shared key obtainment unit 1308a; and the second shared key obtainment unit 1309a, and the components which are common among the receiving devices 13a to 13n include: the individual information receiving unit 1301; the common information receiving unit 1306; and the output unit 1310.

[0093] (1) Individual Information Receiving Unit 1301

In the case where the individual information receiving unit 1301 receives an individual information group EMMG from the server 12, it extracts the first individual information EMMI and the second individual information EMMII based on the individual information identifiers EMMIDI and EMMIDII which are included in the received individual information group EMMG, and outputs the first individual information EMMI to the first individual intermediate group obtainment unit 1302a, and the second individual information EMMII to the second individual intermediate key group obtainment unit 1303a.

[0094] (2) First Individual Intermediate Key Group Obtainment Unit 1302a

In the case where the first individual intermediate key group obtainment unit 1302a receives the first individual information EMMI from the individual information receiving unit 1301, it obtains a receiving device identifier AIDa, an individual key IKa and a first encrypted individual intermediate key group set ENCMKIGSa from the individual key storage unit 1304a as shown in FIG. 28 first. After that, it obtains a term identifier (such as PID_i: PID_i is one of PID₁ to PID_k) and an encrypted term key ENCPKa corresponding

to the receiving device identifier AIDa which has been stored in the individual key storage unit 1304a. After that, it decrypts the encrypted term key ENCPKa based on the individual key IKa stored in the individual key storage unit 1304, and obtains the term key
5 PK_i corresponding to the term identifier PID_i. After that, it obtains the first encrypted intermediate key group (such as ENCMKIGa_i: ENCMKIGa_i is one of ENCMKIGa_1 to ENCMKIGa_k) corresponding to a term identifier (example: PID_i which is one of PID_1 to PID_k) in the first individual information EMMI, from
10 among the first encrypted individual intermediate key group set ENCMKIGSa as shown in FIG. 29, decrypts the first encrypted individual intermediate key group based on the term key PK_i, and obtains the first individual intermediate key group MKIGa as shown in FIG. 30. After that, it stores the decrypted first individual
15 intermediate key group MKIGa in the individual intermediate key storage unit 1305a.

[0095] (3) Second Individual Intermediate Key Group Obtainment Unit 1303a

In the case where the second individual intermediate key
20 group obtainment unit 1303a receives the second individual information from the individual information receiving unit 1301, it obtains a receiving identifier AIDa and an individual key IKa from the individual key storage unit 1304a as shown in FIG. 28 first. After that, it obtains the second encrypted individual intermediate
25 key group ENCMKIIGa corresponding to the receiving device identifier AIDa which has been stored in the individual key storage unit 1304, from the received second individual information EMMII. After that, it decrypts the second encrypted individual intermediate key group ENCMKIIGa based on the individual key IKa, and obtains
30 the second individual intermediate key group MKIIGa. After that, it stores the second individual intermediate key group MKIIGa in the individual intermediate key storage unit 1305a.

[0096] (4) Individual Key Storage Unit 1304a

As shown in FIG. 28, the individual key storage unit 1304a holds the receiving device identifier AIDa, the individual key IKa, and the first encrypted individual intermediate key group set ENCMKIGSa. It is possible to access the individual key storage unit 1304a through the first individual intermediate key group obtainment unit 1302a and the second individual intermediate key group obtainment unit 1303a. Also, the receiving device identifier AIDa is, for example, a natural number, and it takes a value which is different from the respective receiving device identifiers AIDb to AIDn. The individual key IKa is, for example, a key of DES encryption method described in the Non-patent Reference 2. The individual key IKa has been generated in advance using, for example, a random number embedded in the individual key IKa, and it takes a value which is different from the individual keys IKb to IKn.

[0097] Note that the first encrypted individual intermediate key group set ENCMKIGSa which is stored in this individual key storage unit 1304a has a random number which has been embedded by means that the key distribution center 11 performing the following method.

[0098] Two individualized variables x and y which satisfy a previously provided individualized variable generation equation " $x*y=c_1 \bmod N$ " are generated for the first system secret variables s_1, t_1, u_1, v_1 and c_1 which correspond to the term identifier PID_1. Here, as a method for generating these two individualized variables x and y , for example, there is a method for generating an individualized variable (example: x) using a random number, and substituting the value to the individualized variable generation equation so as to obtain the other individualized variable (example: y). When selecting one random individualized variable x , the corresponding individualized variable y is surely present. Also,

these individualized variables x and y are natural numbers of 128 bits, and "*" represents multiplication. For example, $2*5$ means 10, and it is used in the same meaning hereinafter. After that, four first individual intermediate keys $mkI1$, $mkI2$, $mkI3$ and $mkI4$ are generated using the individualized variables x and y based on the previously provided four first individual intermediate key generation equations " $mkI1=s_1*x \bmod N$ ", " $mkI2=t_1*y \bmod N$ ", " $mkI3=-u_1*x \bmod N$ " and " $mkI4=-v_1*y \bmod N$ ". After that, it generates the first individual intermediate key group $MKIGa$ as shown in FIG. 30 which is composed of the four first individual intermediate key group $mkI1$, $mkI2$, $mkI3$ and $mkI4$. After that, it encrypts the first individual intermediate key group $MKIGa$ in association with the term identifier PID_1 based on the term key PK_1 which is held by the key distribution center 11, and generates a first encrypted individual intermediate key group $ENCMKIGa$. Likewise, individualized variables x and y are generated for the others: the first system secret variables s_2 to s_k ; the second system secret variables t_2 to t_k ; the third system secret variables u_2 to u_k ; the fourth system secret variables v_2 to v_k and the fifth system secret variables c_2 to c_k . Also, the followings are generated based on the first individual intermediate key generation equation: the first individual intermediate key $mkI1_2$ to $mkI1_k$, $mkI2_2$ to $mkI2_k$, $mkI3_2$ to $mkI3_k$, and $mkI4_2$ to $mkI4_k$. After that, it generates the first individual intermediate key group $MKIGa_2$ which is composed of the first individual intermediate keys, the first individual intermediate key group equals to $(mkI1_2||mkI2_2||mkI3_2||mkI4_2)$, $MKIa_3$, ..., $MKIa_k$. After that, it encrypts the first individual intermediate key group $MKIGa_2$ in association with the respective term identifiers PID_2 , ..., PID_k based on the term keys PK_2 , ..., PK_n , and generates the first encrypted individual intermediate key group $ENCMKIGa_2$, ... $ENCMKIGa_k$. Lastly, a value which is obtained by combining the

sets of an encrypted first individual intermediate key group and an associated term identifier is previously embedded as an encrypted first individual intermediate key group set ENCMKIGSa, the value being shown in FIG. 29 and represented as {(ENCMKIGa_1, PID_1)|| (ENCMKIGa_2, PID_2)||, ... || (ENCMKIGa_k, PID_k)}. Note that, the respective encrypted first individual intermediate key group sets (ENCMKIGSa to ENCMKIGSn) are made to be the values which differ among the receiving devices 13a to 13n. This can be realized by, for example, generating such individualized variables (x, y) which are different among the respective receiving devices 13a to 13n and the respective term identifiers PID_1 to PID_k, and using them.

[0099] (5) Individual Intermediate Key Storage Unit 1305a

As shown in FIG. 31, the individual intermediate key storage unit 1305a holds a first individual intermediate key group MKIGa and a second individual intermediate key group MKIIGa. It is possible to access this individual intermediate key storage unit 1305a through first individual intermediate key group obtainment unit 1302a and the second individual intermediate key group obtainment unit 1303a.

[0100] (6) Common information Receiving Unit 1306

In the case where the common information receiving unit 1306 receives common information ECM from the server 12, it outputs the received common information ECM to the second selection unit 1307a.

[0101] (7) Second Selection Unit 1307a

In the case where the second selection unit 1307a receives common information ECM from the common information receiving unit 1306, it determines which one of the first common information ECMI and the second common information ECMII is the common information ECM, based on the common information identifier (ECMIDI or ECMIDII) included in the common information ECM. In

the case where the common information ECM is the first individual information ECMI, it obtains the first individual intermediate key group MKIGa from the individual intermediate key storage unit 1305a, and outputs the first common information ECMI and the first individual intermediate key group MKIGa to the first shared key obtainment unit 1308a. In contrast, in the case where the common information ECM is the second individual information ECMII, it obtains the second individual intermediate key group MKIIGa from the individual intermediate key storage unit 1305a, and outputs the second common information ECMII and the second individual intermediate key group MKIIGa to the second shared key obtainment unit 1309a.

[0102] (8) First Shared Key Obtainment Unit 1308a

In the case where the first shared key obtainment unit 1308a receives the first individual intermediate key group MKIGa and the first common information ECMI from the second selection unit 1307a, it extracts the time variable PRG from the first common information ECMI first. After that, it extracts time variables r1, r2, r3 and r4 from the time variable group PRG, and then extracts the first individual intermediate keys mkI1, mkI2, mkI3 and mkI4 from the first individual intermediate key group MKIGa. After that, it generates a shared intermediate key SMK based on the previously provided receiving device shared intermediate key generation equation " $SMK = (r1 + mkI1) * (r1 + mkI2) + (r1 + mkI3) * (r1 + mkI4) \bmod N$ ". After that, it extracts an encrypted shared key ENCSK from the first common information ECMI, decrypts the encrypted shared key ENCSK based on the generated shared intermediate key SMK, and obtains the shared key SK. After that, it outputs the shared key SK to the output unit 1310.

[0103] (9) Second Shared Key Obtainment Unit 1309a

In the case where the second shared key obtainment unit 1309a receives the second individual intermediate key group

MKIIGa and the second common information ECMII from the second selection unit 1307a, it extracts the second encrypted shared keys ENCSK1, ENCSK2, ENCSK3, ENCSK4, ENCSK 5 and ENCSK 6 from the second encrypted shared key group ENCSKG. After that, it
5 selects the encrypted sentence obtained by encrypting the shared key SK using the second system secret key from among the second encrypted shared keys ENCSK1, ENCSK2, ENCSK3, ENCSK4, ENCSK 5 and ENCSK 6, based on the second system secret key included in the second individual intermediate key group MKIIGa, decrypts the
10 selected one of encrypted sentences, and obtains the shared key SK. After that, it outputs the shared key SK to the output unit 1310. Note that, as a method for selecting one encrypted sentence from among the second encrypted shared keys ENCSK1, ENCSK2, ENCSK3, ENCSK4, ENCSK 5 and ENCSK 6, a method of selecting one
15 from among the second encrypted shared keys ENCSK1 to ENCSK6 based on the second system secret key identifiers so that: (a) the second system secret key identifiers are included in the second encrypted shared key group ECSKG in the second common information generation unit 126, the second system secret key
20 identifiers being intended for identifying the second system secret keys which have been used for encrypting the shared keys and being associated with the second encrypted shared keys respectively; and likewise, (b) the second system secret key identifiers which are associated with the included second system keys are included in the
25 second individual intermediate key group MKIIGa.

[0104] (10) Output Unit 1310

In the case where the output unit 1310 receives a shared key SK from one of the first shared key obtainment unit 1308a and the second shared key obtainment unit 1309a, it outputs the received
30 shared key SK to outside.

[0105] <Operation of Receiving Device 13>

The structure of the receiving device 13a has been described

up to this point, and here will be described the operation of the receiving device 13a. First, how the receiving device 13a performs the operation of obtaining the first individual intermediate key group MKIGa and the second individual intermediate key group MKIIGa at the time of receiving an individual information group EMMG will be described with reference to the flow chart shown in FIG. 32. Next, how the receiving device 13a performs the operation of obtaining the first individual intermediate key group MKIGa and the second individual intermediate key group MKIIGa at the time of receiving common information ECM will be described with reference to the flow chart shown in FIG. 33.

[0106] <Operation Performed when Individual Information Group EMMG has been Received from Key Distribution Center 11>

The individual information receiving unit 1301 which has received the individual information group EMMG from the key distribution center 11 extracts the first individual information EMMI and the second individual information EMMII from the received individual information group EMMG (S1301).

The individual information receiving unit 1301 outputs the first individual information EMMI to the first individual intermediate key group obtainment unit 1302a, and outputs the second individual information EMMII to the second individual intermediate obtainment unit 1303a (S1302).

The first individual intermediate key group obtainment unit 1302a which has received the first individual information EMMI obtains a receiving device identifier AIDa, an individual key IKa, and a first encrypted individual intermediate key group set ENCMKIGSa from the individual key storage unit 1304a (S1303).

The first individual intermediate key group obtainment 1302a obtains a term identifier PID_i and the encrypted term key ENCPKa corresponding to the receiving device identifier AIDa which has been stored in the individual key storage unit 1304 (S1304).

The first individual intermediate key group obtainment unit 1302a decrypts the encrypted term key ENCPKa based on the individual key IKa which has been stored in the individual key storage unit 1304, and obtains the term key PK_i (S1305).

5 The first individual intermediate key group obtainment unit 1302a obtains the encrypted first individual intermediate key group corresponding to the term identifier PID_i in the first individual information EMMI from among the first encrypted individual intermediate key group set ENCMKIGSa, decrypts the first
10 encrypted individual intermediate key group based on the term key PK_i, and obtains the first individual intermediate key group MKIGa (S1306).

The first individual intermediate key obtainment unit 1302a stores the decrypted first individual intermediate key group MKIGa
15 in the individual intermediate key storage unit 1305a (S1307).

The second individual intermediate key group obtainment unit 1303a which has received the second individual information EMMII from the individual information receiving unit 1301 obtains the receiving device identifier AIDa and the individual key IKa from
20 the individual key storage unit 1304a (S1308).

The second individual intermediate key group obtainment unit 1303a obtains the second encrypted individual intermediate key group ENCMKIIGa corresponding to the received device identifier AIDa which has been stored in the individual key storage unit 1304
25 from the received second individual information EMMII (S1309).

The second individual intermediate key obtainment unit 1303a decrypts the second encrypted individual intermediate key group ENCMKIIGa based on the individual key IKa (S1310).

The second individual intermediate key group obtainment
30 unit 1303a stores the decrypted second individual intermediate key group MKIIGa in the individual intermediate key storage unit 1305a (S1311).

<<Operation Performed when Common information Group ECM has been Received from Server 12>>

The common information receiving unit 1306 which has received the common information ECM from the server 12 outputs
5 the received common information ECM to the second selection unit 1307a (S1351).

The second selection unit 1307a which has received the common information ECM from the common information receiving unit 1306 obtains the common information identifier included in the
10 common information ECM. In the case where the common information identifier is ECMIDI, it considers the common ECM as the first common information ECMI, and obtains the first individual intermediate key group MKIGa from the individual intermediate key storage unit 1305a. It outputs the first individual intermediate key
15 group MKIGa and the first common information ECMI to the first shared key obtainment unit 1308a, and goes to Step 1352. In the case where the common information identifier is ECMIDII, it considers the common information ECM as the second common information ECMII, and also obtains the second individual
20 intermediate key group MKIIGa from the individual intermediate key storage unit 1305a. It outputs the second individual intermediate key group MKIIGa and the second common information ECMII to the second shared key obtainment unit 1309a, and goes to Step 1356 (S1352).

25 The first shared key obtainment unit 1308a which has received the first individual intermediate key group MKIGa and the first common information ECMI, extracts a time variable PRG from the first common information ECMI, and then extracts the time variables r1, r2, r3 and r4 from the time variable group PRG. After
30 that, it extracts the first individual intermediate keys mkI1, mkI2, mkI3 and mkI4 from the first individual intermediate key group MKIa. After that, it calculates a shared intermediate key SMK

based on the previously provided receiving device shared intermediate key generation equation " $SMK=(r1 + mkI1)*(r2 + mkI2)+(r3+mkI3)*(r4+mkI4) \bmod N$ " (S1353).

5 The first shared key obtainment unit 1308a extracts an encrypted shared key ENCSK from the first common information ECMI, decrypts the encrypted shared key ENCSK based on the generated shared intermediate key SMK, and obtains the shared key SK (S1354).

10 The first shared key obtainment unit 1308a outputs the shared key SK to the output unit 1310, and goes to Step 1358 (S1355).

The second shared key obtainment unit 1309a which has received the second individual intermediate key group MKIIGa and the second common information ECMII extracts, from the encrypted
15 shared key group ENCSKG, the second encrypted shared keys ENCSK1, ENCSK2, ENCSK3, ENCSK4, ENCSK5, and ENCSK6. After that, it decrypts one encrypted sentence corresponding to one of the six second encrypted shared keys ENCSK1, ENCSK2, ENCSK3, ENCSK4, ENCSK5, and ENCSK6 (S1356).

20 The second shared key obtainment unit 1309a outputs the shared key SK to the output unit 1310 (S1357).

In the case where the output unit 1310 receives a shared key SK from one of the first shared key obtainment unit 1308a and the second shared key obtainment unit 1309a, it outputs the received
25 shared key SK to the outside (S1358).

The structure and the operation of the receiving device 13a which is a component of the key distribution system 1 have been described up to this point. Note that the difference between the receiving device 13a and the receiving devices 13b to 13n is as
30 follows.

[0107] (i) The respective receiving devices 13a to 13n have a different receiving device identifier, a different individual key, and a

different first encrypted intermediate key group set which are obtained from the individual key storage unit 1304a in order that the first individual intermediate key group obtainment unit 1302a obtains the first individual intermediate key group.

5 (ii) The respective receiving devices 13a to 13n have a different receiving device identifier and an individual key which are obtained from the individual key storage unit 1304a in order that the second individual intermediate key group obtainment unit 1303a obtains the second individual intermediate key group.

10 [0108] (iii) The respective receiving devices 13a to 13n have different receiving device identifiers (AIDa to AIDn), individual keys (IKa to IKn), and first encrypted individual intermediate key group sets which are stored in the individual key storage unit 1304a.

[0109] (iv) The respective receiving devices 13a to 13n have
15 different first individual intermediate key groups and different second individual intermediate key groups which are stored in the individual intermediate key storage unit 1305a.

[0110] (v) The respective receiving devices 13a to 13n have
20 different first individual intermediate key groups and second individual intermediate key groups which are obtained from the individual intermediate key storage unit 1305a by the second selection unit 1307a.

[0111] (vi) The receiving devices 13a to 13n each has a different
25 first individual intermediate key group which is used at the time of obtaining a shared key SK in the first shared key obtainment unit 1308a.

[0112] (vii) The receiving devices 13a to 13n each has a different
30 second individual intermediate key group which is used at the time of obtaining a shared key SK in the second shared key obtainment unit 1309a.

[0113] <Operation Verification of First Embodiment>

All the receiving devices 13a to 13n can derive the shared

keys SK with a same value in the first embodiment even though one of the first individual intermediate key groups MKIGa to MKIGn and one of the second individual intermediate key groups MKIIGa to MKIIGn each of which takes a different value are assigned to the respective receiving devices 13a to 13n. The reason will be described.

[0114] First, the case of using the first common information ECMI and the first individual intermediate key groups MKIGa to MKIGn will be described. The respective first individual intermediate key groups MKIGa to MKIGn are composed of the first individual intermediate keys mkI1, mkI2, mkI3 and mkI4 which satisfy the previously provided four first individual intermediate key generation equations. Also, the time variable group PRG is generated so that it satisfies the four time variable generation equations. In this way, the receiving device shared intermediate key generation equation can be transformed as follows.

$$\begin{aligned}
 [0115] \quad & \text{SMK} = (r1 + mkI1) * (r2 + mkI2) + (r3 + mkI3) * (r4 + mkI4) \\
 & = \{s * (z + x) + v * m\} * \{t * (w + y) + u * n\} + \{u * (z - x) + t * m\} * \{v * (w - y) + s * n\} \\
 & = \{s * (z + x) * t * (w + y) + u * (z - x) * v * (w - y)\} + \{u * n * s * (z + x) + \\
 & \quad + v * m * t * (w + y) + s * n * u * (z - x) + t * m * v * (w - y)\} + u * v * m * n + s * t * m * n
 \end{aligned}$$

Here, by using the condition of "x*y=c", the above equation can be transformed to

$$= 2 * s * t * (z * w + c * n * m) + 2 * (u * s * n * z + t * v * m * w)$$

This equation is composed of only the parameters which are common in the respective receiving devices 13a to 13n (in other words, the individualized variables x and y are not included). Therefore, in all the respective receiving devices 13a to 13n the common value is derived from the shared intermediate keys SMK. Also, this matches the server shared intermediate key generation equation "SMK=2*s*t*(z*w+c*n*m)+2*(u*s*n*z+t*v*m*w)".

[0116] Next, the case where the second common information ECMII and the second individual intermediate groups MKIIGa to MKIIGn will be described. The second individual intermediate key groups MKIIGa to MKIIGn are composed of one of the second system secret keys which have been previously provided (they are six in the case of first embodiment). Also, the second common information ECMII includes the encrypted sentence of the shared key SK which has been encrypted using the respective second system secret keys. Therefore, in all of the receiving devices 13a to 13n which hold one of the second system secret keys, the shared key SK can be derived.

[0117] <Effect of First Embodiment>

In the first embodiment of the present invention, the shared keys SK with a same value which are owned by all of the receiving devices are generated from each of the first individual intermediate key groups and the second individual intermediate key groups which are unique to each receiving device. In this way, if individual information of the first individual intermediate key groups and the second individual intermediate key groups is forged, it becomes possible to identify the receiving device as the leakage source using the other individual intermediate keys, and thus the safety can be improved.

[0118] (Second Embodiment)

The key distribution system 2 as an embodiment of the present invention will be described. In the key distribution system 1 in the first embodiment, a shared key has been obtained by selecting one of the two shared key obtainment methods at the time when the respective output devices 13a to 13n receive the common information ECM. However, in the content distribution system 2 in the second embodiment, a shared key is obtained using both the two shared key obtainment methods at the time of receiving the ECM. In this regards, this second embodiment is much different from the

first embodiment.

[0119] Details of the content distribution system 2 which is an embodiment of the content distribution system of the present invention will be described below.

5 [0120] <Structure of Content Distribution System 2>

As shown in FIG. 34, the key distribution system 2 includes: (a) a communication channel 10 which is the same as the one in the first embodiment; and (b) a key distribution center 21, a server 22 and receiving devices 22a to 22n which are different from the ones
10 in the first embodiment. The roles of the respective components are the same as the ones of the key distribution center 11, the server 12 and the output devices 13a to 13n in the key distribution system 1 which is the first embodiment.

[0121] Details of the key distribution system 2 which is an
15 embodiment of the key distribution system of the present invention will be described below.

[0122] Details of these components will be described. First, the structures and the operations of the key distribution center 21, the server 22 and the receiving devices 23a to 23n will be described with
20 reference to figures.

[0123] <Structure of Key Distribution Center 21>

As shown in FIG. 35, the key distribution center 21 includes: a fourth control unit 211; a third individual information generation unit 212; a receiving device information storage unit 113; a system
25 secret variable group set sending unit 215; and an individual information group distribution unit 216. Note that the receiving device information storage unit 113 is the same as the receiving device information storage unit 113 in the key distribution system 2 in the first embodiment, and thus the description will be omitted.

30 [0124] (1) First Control Unit 211

In the case where the first control unit 211 satisfies the previously provided individual information update condition, and in

the case where the key distribution center 23 starts its operation, it outputs the third individual information generation request REQEMMIII to the third individual information generation unit 212. For example, in the case where the individual information update condition is "for every term which is specified (example: everyday and every year)", the counter can be updated by means that the first control unit 211 has a counter. In the case where the individual information update condition is "when a signal from outside is received", the counter can be updated by the first control unit 211 which has a receiving unit for receiving a signal from outside.

[0125] (2) Third Individual Information Generation Unit 212

As shown in FIG. 36, the third individual information generation unit 212 includes: a third system secret variable group generation unit 2121; and a first intermediate key group generation unit 2122.

[0126] (2-1) Third System Secret Variable Group Generation Unit 2121

In the case where the third system secret variable group generation unit 2121 receives the third individual information generation request REQEMMIII from the first control unit 211, it generates the first system secret variable groups {SPGI1, SPGI2, SPGI3, SPGI4, SPGI5 and SPGI6} for the respective six first system secret variable group identifiers SPGIID1 to SPGIID6. Note that, as to the structure of the respective first system secret variable groups SPGIi (SPGI1 to SPGI6), the respective groups are composed of five first system secret variables (s_i, t_i, u_i, v_i, c_i : i is 1 to 6) like in the key distribution system 1 of the first embodiment as shown in FIG. 5. Also, the respective first system secret variables SPGI1 to SPGI6 are generated in advance so that they satisfy the first system secret variable generation equation " $s_i * t_i = u_i * v_i \bmod N$: i is 1 to 6". For example, the five first system secret variables and the modulus N are natural numbers of, for example, 128 bits. Also, the

value of the modulus N here is the same as the value of the modulus N which has been previously provided, as the common value, to the later-described third common information generation unit 225 and third shared key generation unit 2308a, and it is, for example,
5 $2^{\{128\}}$. Here, “^” is power operation. For example, $2^{\{4\}}$ means 16, and it is used in the same meaning hereinafter.

The first system secret variable group identifiers SPGID1 to SPGIID6 are identifiers which are associated with the respective first system secret variable groups SPGI1 to SPGI6, and for example,
10 they are respectively different natural numbers. For example, the six first system secret variable group identifiers SPGIID1 to SPGIID6 may be natural numbers of 1 to 6 or random numbers. Non-patent Reference 3 describes in detail the method of generating random numbers. After that, as shown in FIG. 37, it generates the third
15 system secret variable group SPGIII which is composed of the six sets of a first system secret variable group identifier and a first system secret variable group, the sets being {SPGIID1, SPGI1}, {SPGIID2, SPGI2},..., {SPGIID6, SPGI6}, and outputs them to the third system secret variable group set sending unit 215 and the first
20 intermediate key group generation unit 2212.

[0127] (2-2) First Intermediate Key Group Generation Unit 2122

In the case where the first intermediate key group generation unit 2122 receives the third system secret variable group SPGIII from the third system secret variable group generation unit 2121, it
25 accesses the receiving device information storage unit 113, and obtains the receiving device identifiers AIDa to AIDn. After that, it firstly selects, for the receiving device identifier AIDa, one first system secret key group from among the six first system secret key groups SPGI1 to SPGI6 which are included in the third system secret
30 variable groups SPGIII. As an example method of selecting a first system secret key group, there is a method of selecting one at random, and this can be realized using a random number. Here, as

an example, it is assumed that the key selected for the receiving device identifier AIDa is considered as the first secret variable SPGIi (SPGIi is one of the SPGI1 to SPGI6) and that the first secret variable SPGIi is composed of the six first system secret variables s_i, t_i, u_i, v_i and c_i. After that, it generates two individualized variables x and y which satisfy a previously provided individualized variable generation equation " $x*y=c_i \bmod N$ " based on the six first system secret variables s_i, t_i, u_i, v_i and c_i. Here, as an example method of generating two individualized variables x and y, there is a method of generating them using random numbers. Also, the individualized variables x and y are, for example, natural numbers of 128 bits. Also, "*" represents multiplication". For example, $2*5$ means 10, and it is used in the same meaning hereinafter. As an example method of calculating these individualized variables x and y, there is a method of generating an individualized variable x as a random integer value, by substituting the individualized variable x in the individualized variable generation equation " $x*y=c_i \bmod N$ " so as to calculate the other individualized variable y. When a random individualized variable x is selected, the corresponding individualized variable y is surely present. After that, it generates four first individual intermediate keys mkI1, mkI2, mkI3 and mkI4 using the individualized variables x and y based on the previously provided four first individual intermediate key generation equations " $mkI1=s_i*x \bmod N$ ", " $mkI2=t_i*y \bmod N$ ", " $mkI3=-u_i*x \bmod N$ ", and " $mkI4=-v_i*y \bmod N$ ". After that, it generates the first individual intermediate key group MKIGa which is composed of the four first individual intermediate keys mkI1, mkI2, mkI3 and mkI4 as shown in FIG.30. After that, it encrypts the first individual intermediate key group MKIGa based on the individual key IKa, considers the encrypted sentence as the first encrypted individual intermediate key group ENCMKIGa= $Enc(IKa, MKIGa)$, and associates it with the first system

secret variable group identifier SPGIIDi (SPGIIDi is one of SPGIID1 to SPGIID6 corresponding to the receiving device identifier AIDa and the first secret variable SOGIi. After that, as also to the other receiving device identifiers AIDb to AIDn, it considers the encrypted sentence as the first encrypted individual intermediate key groups ENCMKIGb, ... ENCMKIGn, and associates them with the respective receiving device identifiers AIDb to AIDn and the first system secret variable group identifier SPGIIDi. After that, it generates the third individual information EMMIII which is composed of one of the receiving device identifiers AIDa to AIDn, one of the first encrypted individual intermediate key groups ENCMKIGa to ENCMKIGn and one of the first system secret variable group identifiers, and outputs the third individual information EMMIII to the individual information group distribution unit 216. Here, the encryption algorism which is used for encrypting the first individual intermediate key group is, for example, a DES encryption method which is disclosed in Non-patent Reference 2. It uses the same method as the method of decryption algorism which is used at the time of decrypting the first encrypted individual intermediate key in the third individual intermediate key group obtainment unit 1303a of the later-described receiving devices 23a to 23n.

[0128] (3) System Secret Variable Group Set Sending Unit 215

In the case where the system secret variable group set sending unit 215 receives the third system secret variable group SPGIII from the third system secret variable group selection unit 2121 of the third individual information generation unit 212, it sends the third system secret variable group set SPGIII to the server 22.

[0129] (4) Individual Information Group Distribution Unit 216

In the case where the individual information group distribution unit 216 receives the third individual information EMMIII from the first intermediate key group generation unit 2122 of the third individual information generation unit 212, it distributes

the third individual information EMMIII to the receiving devices 23a to 23n.

[0130] <Operation of Key Distribution Center 21>

The structure of the key distribution center 21 has been described up to this point, and here will be described the operation of the key distribution center 21. Here, how the key distribution center 21 starts its operation when distributing, to the server 22 and the receiving devices 23a to 23n, the information necessary for distributing and receiving a shared key in one of: the case where the previously provided individual information update condition is satisfied; the case where the key distribution center 21 starts its operation; and another case, will be described with reference to the flow chart shown in FIG. 39. Also, how the third individual information generation unit 212 operates when generating the third system secret variable group SPGIII and the third individual information EMMIII will be described with reference to the flow chart shown as FIG. 40.

[0131] <Operation of Key Distribution Center 21 in Distributing Key Information>

The first control unit 211 outputs the third individual information generation request REQEMMIII to the third individual information generation unit 212 (S2101).

The third individual information generation unit 212 generates the third system secret variable group SPGIII and the third individual information EMMIII, outputs the third system secret variable group SPGIII to the third system secret variable group set sending unit 215, and outputs the third individual information EMMIII to the third individual information distribution unit 216, according to the flow chart (which will be described below in detail) shown as FIG. 40 (S2102).

The third system secret variable group sending unit 215 which has received the third system secret variable group SPGIII sends the

third system secret variable group SPGIII to the server 22 (S2103).

The third individual information distribution unit 216 which has received the third individual information EMMIII distributes the third individual information EMMIII to the receiving devices 23a to 23n to complete it (S2104).

<<Operation of Key Distribution Center 21 in Generating Third System Secret Variable Group SPGIIIS and Third Individual Information EMMIII (Detailed Description of Step 2102)>>

The third system secret variable group generation unit 2121 which has received the third individual information generation request REQEMMIII generates the first system secret variable group {SPGI1, SPGI2, SPGI3, SPGI4, SPGI5 and SPGI6} each of which is composed of the five first system secret variables (s_i, t_i, u_i, v_i, c_i: i is 1 to 6), and respectively associates them with the first system secret variable group identifiers SPGIID1 to SPGIID6 (S21021).

The third system secret variable group generation unit 2121 generates the third system secret variable group SPGIII which is composed of the six sets of a first system secret variable group identifier and a first system secret variable group, the sets being {SPGIID1, SPGI1}, {SPGIID2, SPGI2},... {SPGIID6, SPGI6}, and then outputs the third system secret variable group set sending unit 215 and the first intermediate key group generation unit 2212 (S1022).

The first intermediate key group generation unit 2122 which has received the third system secret variable group SPGIII accesses the receiving device information storage unit 113 and obtains the receiving device identifiers AIDa to AIDn (S21023).

The first intermediate key group generation unit 2122 which has received the third system secret variable group SPGIII selects a first system secret key group SPGIi (i is one of 1 to 6) from among the six first system secret key groups SPGI1 to SPGI6 which are

included in the third system secret variable group SPGIII, and extracts five first system secret variables s_i , t_i , u_i , v_i and c_i (S21024).

5 The first intermediate key group generation unit 2122 generates two individualized variables x and y which satisfy the previously provided individualized variable generation equation " $x*y=c_i \bmod N$ " based on the five first system secret variables s_i , t_i , u_i , v_i and c_i (S21025).

10 The first intermediate key group generation unit 2122 generates four first individual intermediate keys $mkI1$, $mkI2$, $mkI3$ and $mkI4$ using the individualized variables x and y based on the previously provided four first individual intermediate key generation equations " $mkI1=s_i*x \bmod N$ ", " $mkI2=t_i*y \bmod N$ ", " $mkI3=-u_i*x \bmod N$ " and " $mkI4=-v_i*y \bmod N$ ". After that, it
15 generates the first individual intermediate key group MKIGa which is made up of the four first individual intermediate keys $mkI1$, $mkI2$, $mkI3$ and $mkI4$ as shown in FIG. 30 (S21026).

The first intermediate key group generation unit 2122 encrypts the first individual intermediate key group based on the
20 individual key, considers the encrypted sentence as the first encrypted individual intermediate key group, and assigns it to the receiving device identifiers to which a first encrypted individual intermediate key group has not yet been assigned (S21027).

In the case where first encrypted individual intermediate key
25 groups are assigned to all the receiving device identifiers AIDa to AIDn, the first intermediate key group generation unit 2122 goes to Step 21029. In the other case where first encrypted individual intermediate key groups are assigned to all the receiving device identifiers AIDa to AIDn, the first intermediate key group generation
30 unit 2122 returns to Step 21024 (S21028).

The first intermediate key generation unit 2122 generates the third individual information EMMIII which is composed of: one of the

receiving device identifiers AIDa to AIDn; one of the first encrypted individual intermediate key groups ENCMKIGa to ENCMKIGn; and the first system secret variable group identifier, and outputs the third individual information EMMIII to the individual information group distribution unit 216 to complete it (S21029).

The structure and the operation of the key distribution center 21 which is a component of the key distribution system 2 have been described up to this point, and consequently the structure and the operation of the server 22 will be described.

[0132] <Structure of Server 22>

As shown in FIG. 41, the server 22 includes: a system secret variable group set receiving unit 221; a system secret variable group storage unit 222; a shared key generation unit 123; a third common information generation unit 225; and a common information distribution unit 227. Note that the shared key generation unit 123 is the same as the shared key generation unit 123 in the key distribution system 1 of the embodiment 1, and thus the description will be omitted.

[0133] (1) System Secret Variable Group Set Receiving Unit 221

In the case where the system secret variable group set receiving unit 221 receives the third system secret variable group set SPGIIIS from the key distribution center 21, it stores the received third system secret variable group set SPGIIIS in the system secret variable group storage unit 222 as shown in FIG. 42, and outputs the shared key generation request REQSK to the shared key generation unit 123.

[0134] (2) System Secret Variable Group Storage Unit 222

The system secret variable group storage unit 222 is for storing the third system secret variable group set SPGIII as shown in FIG. 42.

[0135] (3) Third Common information Generation Unit 225

In the case where the third common information generation

unit 225 receives a shared key SK from the common information generation unit selection unit 124, it accesses the system secret variable group storage unit 222 first, obtains the third system secret variable group SPGIII, and, from among the group, extracts six sets of a first system secret variable identifier and a first system secret variable group. After that, it extracts, for the first set of a first system secret variable identifier SPGIID1 and a first system secret variable group SPGI1, six first system secret variables s_1 , t_1 , u_1 , v_1 and c_1 . After that it generates four random numbers z , w , m and n . Here, as an example method of generating random numbers z , w , m and n , there is a method of generating them using random numbers. Also, the respective random numbers z , w , m and n are natural numbers of 128 bits. After that, it generates four time variables r_1 , r_2 , r_3 and r_4 based on the previously provided four time variable generation equations " $r_1=s_1*z+v_1*m \bmod N$ ", " $r_2=t_1*w+u_1*n \bmod N$ ", " $r_3=u_1*z+t_1*m \bmod N$ ", " $r_4=v_1*w+s_1*n \bmod N$ ". After that it generates the time variable group PRG (this is considered as the time variable PRG1) which is shown in FIG. 20 and is composed of the generated time variables r_1 , r_2 , r_3 and r_4 , and associates the time variable group PRG with the first system secret variable identifier SPGIID1. After that, it generates the shared intermediate key SMK based on the following previously provided server shared intermediate key generation equation:

$$\text{"SMK}=2*s_1*t_1*(z+w+c_1+n*m)+2*(u_1*s_1*n*z+t_1*v_1*m*w) \bmod N\text{"}$$

Lastly, it encrypts the received shared key SK based on the shared intermediate key SMK, generates an encrypted shared key ENCSK (this is considered as the shared intermediate key ENCSK1), and associates the encrypted shared key ENCSK with the first system secret variable identifier SPGIID1 and the time variable group PRG. After that, like in the case of the SPGIID1, it generates time variable

groups PRG2 to PRG6 and encrypted shared keys ENCSK2 to ENCSK6 for the other sets of: one of the first system secret variable identifiers SPGIID2 to SPGIID6; and one of the encrypted shared keys ENCSK2 to ENCSK6. After that, it generates the third common information ECMIII which is shown in FIG. 43 and is composed of the first system secret variable identifiers SPGIID1 to SPGIID6, the time variable groups PRG1 to PRG6 and the encrypted shared keys ENCSK1 to ENCSK6, and outputs it to the common information distribution unit. Here, the encryption algorithm which is used for encrypting the shared key SK is, for example, a DES encryption method, and the method used here is the same as the method of the decryption algorithm which is used for decrypting the encrypted shared key ENCSK in the respective third shared key obtainment units 2308a of the later-described receiving devices 13a to 13n.

[0136] (4) Common information Distribution Unit 227

In the case where the common information distribution unit 227 receives the third common information ECMIII from the third common information generation unit 225, it distributes the third common information EMCIII to the receiving devices 23a to 23n.

[0137] <Operation of Server 22>

The structure of the server 22 has been described up to this point, and here will be described the operation of the server 22. First, how the server 22 operates when receiving the third system secret variable group set SPGIII which is used at the time when the shared keys SK are distributed from the key distribution center 21 will be described with reference to the flow chart shown in FIG. 44. Next, how the server 22 operates at the time of distributing the new shared keys SK to the receiving devices 23a to 23n in one of: the case where it receives the shared key generation request REQSK from the system secret variable group set receiving unit 221; and the case where it satisfies the previously provided shared key update condition, will be described with reference to the flow chart

shown in FIG. 45.

[0138] <<Operation of Server 22 in Receiving Third System Secret Variable Group Set SPGIIIS from Key Distribution Center 21>>

5 The system secret variable group set receiving unit 221 stores the received third system secret variable group set SPGIIIS in the system secret variable group storage unit 222 to complete it (S2202).

10 <<Operation of Server 22 in Distributing New Shared Key SK to Receiving Devices 23a to 23n>>

 The shared key generation unit 123 generates a shared key SK and outputs it to the third common information generation unit 225 (S2251).

15 The third common information generation unit 225 accesses the system secret variable group storage unit 222, obtains the third system secret variable group SPGIII, and from among the group, extracts six sets of a first system secret variable identifier and a first system secret variable group (S2252).

20 The third common information generation unit 225 extracts six first system secret variables s_i , t_i , u_i , v_i and c_i for the one set of a first system secret variable identifier and a system secret variable group for which a time variable group and an encrypted shared key have not yet been generated, and after that, it generates four random numbers z , w , m and n (S2253).

25 The third common information generation unit 225 generates four time variables r_1 , r_2 , r_3 and r_4 based on the previously provided four time variable generation equations " $r_1 = s_i * z + v_i * m \bmod N$ ", " $r_2 = t_i * w + u_i * n \bmod N$ ", " $r_3 = u_i * z + t_i * m \bmod N$ ", " $r_4 = v_i * w + s_i * n \bmod N$ " (S2254).

30 The third common information generation unit 225 generates a time variable group PRG which is composed of the generated time variables r_1 , r_2 , r_3 and r_4 (S2255).

The third common information generation unit 225 generates the shared intermediate key SMK based on the previously provided server shared intermediate key generation equation "SMK=2*s_i*t_i*(z+w+c_i+n*m)+2*(u_i*s_i*n*z+t_i*v_i*m*w) mod N" (S2256).

The third common information generation unit 225 encrypts the received shared key SK based on the shared intermediate key SMK, generates an encrypted shared key ENCSK, and associates the encrypted shared key ENCSK with the first system secret variable identifier SPGIID1 and the time variable group PRG (S2257).

The third common information generation unit 225 generates the time variable groups PRG1 to PRG6 and the encrypted shared keys ENCKS1 to ENCKS6 for the first system secret variable identifiers SPGIID1 to SPGIID6 of all the sets and then goes to Step 2259. In the case where the time variable groups PRG1 to PRG6 and the encrypted shared keys ENCKS1 to ENCKS6 have not yet been generated for the first system secret variable identifiers SPGIID1 to SPGIID6 of all the sets, it returns to Step 2252 (S2258).

The third common information generation unit 225 generates the third common information ECMIII which is composed of the first system secret variable identifiers SPGIID1 to SPGIID6, the time variable groups PRG1 to PRG6, and the encrypted shared keys ENCSK1 to ENCSK6 (S2259).

The common information distribution unit 227 distributes the third common information ECMIII to the receiving devices 23a to 23n to complete it (S2260).

The structure and the operation of the server 22 which is a component of the key distribution system 2 have been described up to this point. Consequently, the structure and the operation of the receiving devices 23a to 23n will be described. First, the structure and the operation of the receiving device 23a will be described, and next, the difference between the receiving device 23a and the other

receiving devices 23b to 23n will be described.

[0139] <Structure of Receiving Device 23a>

As shown in FIG. 46, the receiving device 23a includes: an individual information receiving unit 2301; a third individual intermediate key group obtainment unit 2302a; an individual key storage unit 2304a; an individual intermediate key storage unit 2305a; a common information receiving unit 2306a; a third shared key obtainment unit 2308a; and an output unit 1310. Here, the third individual intermediate key obtainment unit 2302a, the individual key storage unit 2304a, the individual intermediate key storage unit 2305a, the common information receiving unit 2306a and the third shared key obtainment unit 2308a are the components which are unique to the receiving device 23a, and the individual information receiving unit 2301, the output unit 1310 and the receiving devices 23a to 23n are the components common among the receiving devices 23a to 23n.

[0140] (1) Individual Information Receiving Unit 2301

In the case where the individual information receiving unit 2301 receives the third individual information group EMMIII from the server 22, it outputs the received third individual information EMMIII to the third individual intermediate key group obtainment unit 2302a.

[0141] (2) Third Individual Intermediate Key Group Obtainment Unit 2302a

In the case where the third individual intermediate key group obtainment unit 2302a receives the third individual information EMMIII from the individual information receiving unit 2301, it obtains the receiving device identifier AIDa and the individual key IKa from the individual key storage unit 2304a as shown in FIG. 47. After that, it obtains, from the received third individual information EMMIII, the first encrypted intermediate key group ENCMKIGa corresponding to the receiving device identifier AIDa which has been

stored in the individual key storage unit 2304a. After that, it decrypts the first encrypted intermediate key group ENCMKIGa based on the individual key IKa, and obtains the first intermediate key group MKIGa and the first system secret variable group identifier SPGIIDi. Lastly, it stores the first intermediate key group MKIGa and the first system secret variable group identifier SPGIIDi in the individual intermediate key storage unit 2305a as shown in FIG. 48.

[0142] (3) Individual Key Storage Unit 2304a

As shown in FIG. 47, the individual key storage unit 2304a is for holding the receiving device identifier AIDa and the individual key IKa.

[0143] (4) Individual Intermediate Key Storage Unit 2305a

As shown in FIG.48, the individual intermediate key storage unit 2305a is for holding the first individual intermediate key group MKIGa and the first system secret variable group identifier SPGIIDi.

[0144] (5) Common information Receiving Unit 2306a

In the case where the common information receiving unit 2306a receives the third common information ECMIII from the server 22, it accesses the individual intermediate key storage unit 2305a, and obtains the first individual intermediate key group MKIGa and the first system secret variable group identifier SPGIIDi. After that it extracts the time variable group PRGi and the encrypted shared key ENCSKi which match the first system secret variable group identifier SPGIIDi from among the third common information ECMIII. After that, it outputs the first individual intermediate key group MKIGa, the time variable group PRGi, and the encrypted shared key ENCSKi to the third shared key obtainment unit 2308a.

[0145] (6) Third Shared Key Obtainment Unit 2308a

In the case where the third shared key obtainment unit 2308a receives, from the common information receiving unit 2306a, the first individual intermediate key group MKIGa, the time variable

group PRGi, and the encrypted shared key ENCSKi, it extracts the time variables r1, r2, r3 and r4 from the time variable group PRGi. After that, it extracts the first individual intermediate keys mkI1, mkI2, mkI3 and mkI4 from the first individual intermediate key group MKIGa. After that, it generates a shared intermediate key SMK based on the previously provided receiving device shared intermediate key generation equation " $SMK = (r1 + mkI1) * (r1 + mkI2) + (r1 * mkI3) * (r1 + mkI4) \bmod N$ ". After that, it decrypts the encrypted shared key ENCSKi based on the generated shared intermediate key SMK, and obtains the shared key SK. After that, it outputs the shared key SK to the output unit 1310.

[0146] <Operation of Receiving Device 23a>

The structure of the receiving device 23a has been described up to this point, and here will be described the operation of the receiving device 23a. First, how the receiving device 23a operates in obtaining the first individual intermediate key group MKIGa when it has received the third individual information EMMIII will be described with reference to the flow chart shown in FIG. 49. Next, how the receiving device 23a operates in obtaining the shared key SK using the first individual intermediate key group MKIGa when it has received the third common information ECMIII will be described with reference to the flow chart shown in FIG. 50.

[0147] <<Operation of Receiving device 23a in Receiving Third Individual Information EMMIII from Key Distribution Center 21>>

The individual information receiving unit 2301 which has received the third individual information group EMMIII from the key distribution center 21 outputs the third individual information EMMIII to the third individual intermediate key group obtainment unit 2302a (S2301). The third individual intermediate key group obtainment unit 2302a which has received the third individual information EMMIII obtains the receiving device identifier AIDa and the individual key IKa from the individual key storage unit 2304a

(S2302).

The third individual intermediate key group obtainment unit 2302a obtains the first encrypted intermediate key ENCMKIa and the first system secret variable group identifier SPGIIDa which
5 correspond to the receiving device identifier AIDa which has been stored in the individual key storage unit 2304 (S2303).

The third individual intermediate key group obtainment unit 2302a decrypts the first encrypted intermediate key ENCMKIa based on the individual key IKa which has been stored in the individual key
10 storage unit 2304, and obtains the first intermediate key MKIa (S2304).

The third individual intermediate key group obtainment unit 2302a stores the first individual intermediate key group MKIGa and the first system secret variable group identifier SPGIIDa in the
15 individual intermediate key storage unit 2305a to complete it (S2304).

<<Operation of Receiving Device 23a in Receiving Third Common information ECMIII from Server 22>>

The common information receiving unit 2306a which has
20 received the third common information ECMIII from the server 22 obtains the first individual intermediate key group MKIGa and the first system secret variable group identifier SPGIIDa from the individual intermediate key storage unit 2305a (S2351).

The common information receiving unit 2306a extracts, from
25 among the third common information ECMIII, the time variable group PRGi and the encrypted shared key ENCSKi which match the first system secret variable group identifier SPGIIDa corresponding to the first system secret variable group identifier SPGIIDa (S2352).

The common information receiving unit 2306a outputs, to the
30 third shared key obtainment unit 2308a, the first individual intermediate key group MKIGa, time variable group PRGi, and the encrypted shared key ENCSKi (S2353).

The third shared key obtainment unit 2308a extracts time variables r1, r2, r3 and r4 from the time variable group PRGi (S2354).

5 The third shared key obtainment unit 2308a extracts the first individual intermediate keys mkI1, mkI2, mkI3 and mkI4 from the first individual intermediate key group MKIGa (S2355).

The third shared key obtainment unit 2308a generates the shared intermediate key SMK based on the previously provided receiving device shared intermediate key generation equation
10 "SMK=(r1+mkI1)*(r1+mkI2)+(r1+mkI3)*(r1+mkI4) mod N" (S2356).

The third shared key obtainment unit 2308a decrypts the encrypted shared key ENCSKi based on the generated shared intermediate key SMK and obtains the shared key SK (S2357).

15 The third shared key obtainment unit 2308a outputs the shared key SK to the output unit 1310 (S2358).

The output unit 1310 outputs the received shared key SK to the outside when it has received the shared key SK (S2359).

The structure and the operation of the receiving device 23a which is a component of the key distribution system 2 have been described up to this point. Note that the difference between the receiving device 23a and the other receiving devices 23b to 23n is as follows.

[0148] (i) The respective receiving devices 23a to 23n have a
25 different receiving device identifier and a different individual key, which are obtained from the individual key storage unit 2304a in order that the third individual intermediate key group obtainment unit 2302a obtains the third individual intermediate key group.

[0149] (ii) The respective receiving devices 23a to 23n have
30 different receiving device identifiers (AIDa to AIDn) and individual keys (IKa to IKn) which are stored in the individual key storage unit 2304a.

[0150] (iii) The respective receiving devices 23a to 23n have different first individual intermediate key groups and different first system secret variable group identifiers which are stored in the individual intermediate key storage unit 2305a.

5 [0151] (iv) The respective receiving devices 23a to 23n have different first individual intermediate key groups and first system secret variable group identifiers which are obtained from the individual intermediate key storage unit 2305a in the common information receiving unit 2306a.

10 [0152] (v) The respective receiving devices 13a to 13n each has a different first individual intermediate key group which is used at the time of obtaining a shared key SK in the third shared key obtainment unit 2308a.

[0153] <Operational verification of second embodiment>

15 The first individual intermediate key groups MKIGa to MKIGn are respectively assigned to the receiving devices 23a to 23n. However, the shared keys SK with a same value can be derived in all of the respective receiving devices 23a to 23n in the second embodiment. The reason is the same as the reason in the case of
20 the first embodiment.

[0154] <Effect of Second Embodiment>

In the second embodiment of the present invention, it is assumed that the shared keys SK with a same value which are owned by all the receiving devices are generated from the third
25 individual intermediate keys which are unique to the respective receiving devices. In this way, it becomes possible to identify a receiving device which is a leakage source even in the case where the device is an unauthorized device in which a third individual intermediate key has been embedded.

30 [0155] <Variations>

The above-described embodiment is an example embodiment of the present invention. The present invention is not limited to

this embodiment and can be executed in main embodiments without deviating from the scope. The following case is also included in the present invention.

[0156] (1) The communication channel 10 may be a
5 broadcasting network such as ground waves and satellite waves.

(2) As shown in FIG.34, in the first embodiment, the key distribution center 11 may record the system secret variable group set SPGS in the portable medium 15 and distribute the portable medium 15 to the server 12, and the server 12 which has received
10 the portable medium 15 may obtain the system secret variable group set SPGS by reading out the system secret variable group set SPGS which has been stored in the portable medium 15. Here, the portable medium 15 is a mobile recording medium such as a flexible disc, a CD-ROM and a DVD-RAM. In this way, it becomes
15 unnecessary that the key distribution center 11 and the server 12 are connected through the communication channel. Note that this can likewise be realized in the second embodiment.

[0157] (3) The followings may be performed in the first embodiment. The key distribution center 11 also generates an
20 extra first individual intermediate key group and distributes the first individual intermediate key in addition to the system secret variable group SPG to the server 12. The system secret variable group storage unit 122 of the server 12 further stores the first individual intermediate key group. As shown in FIG. 35, the time variable
25 group PRG of the server 12 outputs the time variable group PRG to the shared intermediate key obtainment unit 1252 instead of random numbers z , w , m and n . The shared intermediate key obtainment unit 1252 of the server 12, in the case where it has received the time variable group PRG from the time variable group
30 generation unit 1251, accesses the system secret variable group storage unit 122 first, obtains the first individual intermediate key, and obtains the first individual intermediate keys $mkI1$, $mkI2$, $mkI3$,

and mkI4. Also, the shared intermediate key obtainment unit 1252 extracts the time variables r1, r2, r3 and r4 from among the received time variable group PRG, and then generates the shared intermediate key SMK based on the previously provided receiving device shared intermediate key generation equation
5 "SMK=(r1+mkI1)*(r1+mkI2) +(r1+mkI3)*(r1+mkI4) mod N". In this way, even in the case where the first individual intermediate key group of the server 12 is leaked, it becomes possible to trace the server 12 which has leaked the key. Note that this can likewise be
10 realized in the second embodiment.

[0158] (4) Equations are not limited to the followings which have been described in the first embodiment and in the second embodiment: system secret variable generation equations, individualized variable generation equations, first individual
15 intermediate key generation equations, time variable generation equations, server shared intermediate key generation equations and receiving device shared intermediate key generation equations. Any equations may be available as long as (a) the equation which is obtainable when substituting an individualized variable generation
20 equation, a first individual intermediate key generation equation, and a time variable generation equation into the receiving device shared intermediate key generation equation matches the first shared intermediate key, (b) also, the first individual intermediate key generation equation includes individualized variables x and y,
25 and further (c) the time variable generation equation, the server shared intermediate key generation equation, and the receiving device shared intermediate key generation equation do not include the individualized variables x and y.

[0159] (5) The system secret variable group SPG has been
30 generated using a system secret variable generation equation, but a system secret variable group SPG may be generated using two or more types of system secret variable generation equations, and also,

a system secret variable group SPG may be generated without using a system secret variable generation equation. For example, such a system secret variable group may be random numbers.

[0160] (6) The individualized variables have been generated using an individualized variable generation equation, but individualized variables may be generated using two or more types of individualized variable generation equations, and also, individualized variables may be generated without using an individualized variable generation equation. For example, such individualized variables may be random numbers.

[0161] (7) Intermediate keys have been generated using four first individual intermediate key generation equations, but first individual intermediate keys may be generated using five or more types of first individual intermediate key generation equations, and also, first individual intermediate keys may be generated using three or less types of first individual intermediate key generation equations.

[0162] (8) Time variable group PRG have been generated using four time variable generation equations, but a time variable group PRG may be generated using five or more types of time variable generation equations, and further, a time variable group PRG may be generated without using any time variable generation equation. For example, such a time variable group PRG may be random numbers.

[0163] (9) A shared intermediate key SMK has been calculated using a server shared intermediate key generation equation, but a shared intermediate key SMK may be calculated using two or more types of server shared intermediate key generation equations.

[0164] (10) A shared intermediate key SMK has been calculated using a receiving device shared intermediate key generation equation, but a shared intermediate key SMK may be generated using two or more receiving device shared intermediate key

generation equation.

[0165] (11) As to a receiving device shared intermediate key generation equation, a receiving device shared intermediate key generation equation does not need to be used in all of the receiving
5 devices 13a to 13n or the receiving devices 23a to 23n.

[0166] (12) The respective first individual intermediate key groups MKIGa to MKIGn are composed of four first individual intermediate keys mkI1, mkI2, mkI3 and mkI4 in the first
10 embodiment, but they may be composed of five or more first individual intermediate keys, and they may be composed of three or less first individual intermediate keys.

[0167] (13) A time variable group PRG has been composed of four time variables r1, r2, r3 and r4, but it may be composed of five or more time variables, and it may be composed of three or less time
15 variables.

[0168] (14) The same individual key, first individual intermediate key group and first individual intermediate key group may be assigned to some receiving devices.

[0169] (15) The second system secret key generation unit 1141
20 has generated six second system secret keys k1, k2, k3, k4, k5 and k6 in the first embodiment, but it may generate seven or more second system secret keys, and also, it may generate five or less second system secret keys. For example, the second system secret key generation unit 1141 may generate ten second system secret
25 keys k1, k2, k3, k4, k5, k6, k7, k8, k9 and k10. At this time, the number of second system secret keys which are included in the second system secret variable group SPGII vary. For example, in the case where the second system secret key generation unit 1141 generates ten second system secret keys k1, k2, k3, k4, k5, k6, k7,
30 k8, k9 and k10, the second system secret variable group SPGII includes ten second system secret keys k1, k2, k3, k4, k5, k6, k7, k8, k9 and k10.

[0170] (16) The receiving devices have outputted the shared keys SK in the first embodiment and in the second embodiment. However, a server may input contents from outside, encrypt the contents based on the shared keys SK, and distribute the encrypted contents to the receiving devices, and the receiving devices may receive the encrypted contents, perform decryption based on the shared keys SK, obtain the contents, and output the contents to outside.

[0171] (17) The server 12 in the first embodiment has selected one of the first common information generation unit 125 and the second common information generation unit 126, and has generated one of the first common information ECMI and the second common information ECMII. However, the server 12 may generate the first common information ECMI in the first common information generation unit 125 each time, generate the second common information ECMII in the second common information generation unit 126, and after the generation, select one of the first common information ECMI and the second common information ECMII, and distribute the selected one to the receiving devices 13a to 13n.

[0172] (18) When the key distribution center 11 distributes an individual information group EMMG in the first embodiment, it may distribute it to the receiving devices 13a to 13n at the same time, and also, it may distribute it individually to the respective receiving devices 13a to 13n. Also, when the server 12 distributes the common information ECM, it should be noted that the server 12 may distribute it to the receiving devices 13a to 13n at the same time, and also, it may distribute it individually to the respective receiving devices 13a to 13n.

[0173] (19) The third system secret key group set SPGIIIS includes six first system secret key groups in the second embodiment. However, it may include seven or more first system secret key groups, and it may also include five or less first system

secret key groups.

[0174] (20) When the key distribution center 21 distributes the third individual information group EMMIII in the second embodiment, it may distribute it to the receiving devices 23a to 23n at the same time, and it may also distribute individually to the respective receiving devices 23a to 23n. Also when the server 22 distributes the third common information ECMIII, it should be noted that the server 22 may distribute it to the receiving devices 23a to 23n at the same time, and also, it may distribute it individually to the respective receiving devices 23a to 23n.

[0175] (21) The server 12 has sent the common information ECM to the receiving devices 13a to 13n in the first embodiment. However, it is also possible that the server 12 and the receiving devices 13a to 13n previously hold plural sets of common information ECM and a common information identifier, the server 12 distributes the respective common information identifiers to the receiving devices 13a to 13n, and the receiving devices 13a to 13n obtain the corresponding common information ECM based on the received common information identifiers.

[0176] (22) In the first embodiment, the key distribution center 11 may hold (a) the receiving device identifier and (b) the information corresponding to the first individual intermediate key group and the second individual intermediate key group which have been assigned to the receiving devices corresponding to the receiving device identifier, and may become capable of identifying the receiving device to which the information has been assigned based on one of the first individual intermediate key group and the second individual intermediate key group. In this way, even in the case where an unauthorized receiving device is detected, the receiving device from which a leakage has occurred can be identified based on one of the first individual intermediate key group and the second individual intermediate key group which has been embedded

in the unauthorized receiving device. Note that the corresponding information may be held by the key distribution center 11. Also, the corresponding information may include only a set of: (a) one of the first individual intermediate key group and the second individual intermediate key group; and (b) a receiving device identifier. The same can be realized as well by means that the key distribution center 21 or something other than the key distribution center 21 holds (a) the receiving device identifier and (b) the information corresponding to the first individual intermediate key group and the first system secret variable group identifier which have been assigned to the receiving device corresponding to the receiving device identifier. Further, the corresponding information may include only a set of: (a) one of the first individual intermediate key group and the second individual intermediate key group; and (b) a receiving device identifier.

[0177] (23) In the first embodiment, the key distribution center 11 includes a first individual information generation unit and a second individual information generation unit, but it may include a third individual information generation unit and a fourth individual information generation unit, and another individual information generation unit. The receiving devices 13a to 13n include a first individual intermediate key group obtainment unit and a second individual intermediate key group obtainment unit, but it may include a third individual intermediate key group obtainment unit and a fourth individual intermediate key group obtainment unit, and another individual intermediate key group obtainment unit. The requirements are that the key distribution center 11 and the receiving devices 13a to 13n include the same numbers of individual information generation units and individual intermediate key group obtainment units, and individual information identifiers of the same types.

[0178] (24) In the first embodiment, the server 12 includes the

first common information generation unit and the second common information generation unit. However, the server 12 may include a third common information generation unit and a fourth common information generation unit and another common information generation unit. The receiving devices 13a to 13n include the first shared key obtainment unit and the second shared key obtainment unit. However, the respective receiving devices 13a to 13n may include a third shared key obtainment unit and a fourth shared key obtainment unit and another shared key obtainment unit. The requirements are that the server 12 and the receiving devices 13a to 13n include the same number of common information generation units and shared key obtainment units, and the individual information identifiers of the same types.

[0179] (25) In the first embodiment, term keys PK_1 to PK_k are shared keys in all of the receiving devices 13a to 13n, but the receiving devices each may have an individual key.

[0180] (26) The present invention may be the above-described method. Also, the present invention may be a computer program for realizing the method by a computer, and may be digital signals which are composed of the computer program. Also, the present invention may be the computer program or the digital signals recorded in a computer readable recording medium such as a removable disc, a hard disc, a CD, an MO, a DVD, an SD memory card, a semiconductor memory. Also, the present invention may be the computer program or the digital signals recorded in such a recording medium. Also, the present invention may be communicated as the computer program or the digital signals via an electric communication circuit, a wireless communication circuit, a wired communication circuit, a network represented by the Internet or the like. Also, it is possible that the present invention is a computer system including a micro processor and a memory, and the memory stores the above-described computer program, and the

microprocessor operates according to the computer program. Also, the present invention may be executed by another stand-alone computer system by recording the program and the digital signals in the recording medium and transmitting the recording medium, or
5 transmitting the program or the digital signals via the network or the like.

[0181] (27) These embodiments and the variations may be combined with each other.

10 **Industrial Applicability**

[0182] The key distribution system concerning the present invention provides an effect that makes it possible to trace a cloning source of an unauthorized receiving device even in the case where an attacker has received the individual key of a receiving device and
15 generates the unauthorized receiving device using the individual key, and thus the key distribution system is useful in the case where contents are desired to be distributed safely via a communication channel such as the Internet, and a broadcasting network such as ground broadcasting and satellite broadcasting.